NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

EXPANSION OF THE CENTER FOR NETWORK INNOVATION AND EXPERIMENTATION (CENETIX) NETWORK TO A WORLDWIDE PRESENCE

by

Michael M. Farrell

September 2006

Thesis Advisor:	Alex Bordetsky
Co-Advisor:	Douglas Brinkley

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: Expansion of the Center for Network Innovation and Experimentation (Cenetix) Network to a Worldwide Presence	**5. FUNDING NUMBERS**
6. AUTHOR: Michael M. Farrell	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

This thesis will focus directly on the enhancement of an established Network Operations Center (NOC) and will extend the capabilities of this asset beyond its present scope. By defining the current infrastructure using present network management tools it will provide a better understanding of the present network, as well as enhance management for future field experiments. Finally, extending the CENETIX network via implementation of Virtual Private Networking (VPN) technology will allow other experimental labs who currently utilize the Defense Research Engineering Network (DREN), such as the Lawrence Livermore National Laboratory (LLNL), Biometrics Fusion Center (BFC), Defense Threat Reduction Agency (DTR), Office of Force Transformation (OFT), Coast Guard station (located in Alameda), various other US allied forces, Oversea Partners, etc.) access to current and future field experiments.

14. SUBJECT TERMS Virtual Private Network, IPSec, Encrypted Tunnels, CENETIX, Remote Access	**15. NUMBER OF PAGES** 95
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EXPANSION OF THE CENTER FOR NETWORK INNOVATION AND EXPERIMENTATION (CENETIX) NETWORK TO A WORLDWIDE PRESENCE

Michael M. Farrell
Captain, United States Marine Corps
B.B.A., Morehead State University, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2006

Author: Captain Michael M. Farrell

Approved by: Dr. Alex Bordetsky
Thesis Advisor

Dr. Douglas Brinkley
Co-Advisor

Dr. Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis will focus directly on the enhancement of an established Network Operations Center (NOC) and will extend the capabilities of this asset beyond its present scope. By defining the current infrastructure using present network management tools it will provide a better understanding of the present network, as well as enhance management for future field experiments. Finally, extending the CENETIX network via implementation of Virtual Private Networking (VPN) technology will allow other experimental labs who currently utilize the Defense Research Engineering Network (DREN), such as the Lawrence Livermore National Laboratory (LLNL), Biometrics Fusion Center (BFC), Defense Threat Reduction Agency (DTR), Office of Force Transformation (OFT), Coast Guard station (located in Alameda), various other US allied forces, Oversea Partners, etc.) access to current and future field experiments.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The love and gratitude that my wife and children have extended during my course of study has been tremendous. I will forever be grateful to them, as well as my parents who have taught me that perseverance will always be rewarded in the end.

I would also like to thank Dr. Bordetsky and Dr. Brinkley for their support and friendship while working on this work.

THIS PAGE INTENTIONALLY LEFT BLANK

I. CENETIX LAB HISTORY

A. BRIEF HISTORY OF CENETIX LAB

The Center for Network Innovation and Experimentation (CENETIX) has gone through multiple changes since its inception in 2001. These changes have been productive in supporting advanced studies of wireless networking and unmanned vehicles by providing a means for students to perform hands-on thesis research during their studies while at NPS.

CENETIX has its beginning in developing and testing un-manned aerial vehicles (UAV) which would improve the capability of rescuing downed pilots, to conducting surveillance, targeting and acquisition networking (STAN). From that, the CENETIX testbed facility has evolved to a more robust quarterly experimentation cycle which focuses on emerging collaborative architectures as well as adaptive management of sensor-unmanned vehicle networks.

The CENETIX testbed continues where the Global Information Grid Applications (GIGA) Lab has conducted exercises in past Tactical Network Topology (TNT) experiments. External agents who have participated or are working directly with faculty and students include: Lawrence Livermore National Lab (LLNL), Biometrics Fusion Center (BFC), Massachusetts Institute of Technology (MIT), Stanford University, University of California – Santa Barbara (UCSB), and various military agencies (both U.S. and allied) around the world. Currently operations at Camp Roberts and the Naval Post Graduate School locations have been limited to a geographic area, and have presented limitations for those external agencies who wish to

participate. The need for those external agencies the ability to control, observe and participate in future experiments is critical to the success or any new concepts to be tested.

These past experiments conducted from the CENETIX test facilities have proven vital to various Department of Defense (DoD) agencies, combatant commands, and various international allies. This interest has transpired to funding by these agencies, and will continue to allow both faculty and students the opportunity to conduct future experiments with the needs of the customer in mind. Currently the primary funding agencies for the CENETIX testbed facility include:

- CDTEMS (Congressional Funding): FY03 = $1M, FY04=$2M, FY05=$1.75M
- USSOCOM: FY05 = $1. 96M (Light Reconnaissance Vehicle), FY06 (JMUST)

The establishment of a testbed facility, located at Naval Post Graduate School (NPS), which could be utilized by both the trainer and the student, provides a tremendous opportunity to develop, test, and enhance new technologies that are required in the changing tactical environments of the 21st Century. From its inception the CENETIX testbed has maintained three primary objectives:

- Provide an opportunity for NPS students and faculty to demonstrate and evaluate their latest technologies in an operational environment and provide the operational community the opportunity to utilize and experiment with these technologies.
- Take advantage of operational experiences of NPS students.
- Provide the Military, National Laboratories, DoD Contractors, and Universities the opportunity to

test and evaluate latest S&T in operational environment; small, focused field experiments with well-defined measures of performance

B. HOW CENETIX COMMUNICATES

CENETIX is based aboard NPS in Monterey, California and maintains the Global Information Grid Applications and Operations Code Lab (GIGA Lab). Through the efforts of NPS faculty, staff, and students, CENETIX implements an 802.16 Orthogonal Frequency Division Multiplexing (OFDM) wireless network connecting CENETIX facilities within the Monterey Area to experimentation facilities located about one hundred miles to the south at the Camp Roberts National Guard Base.

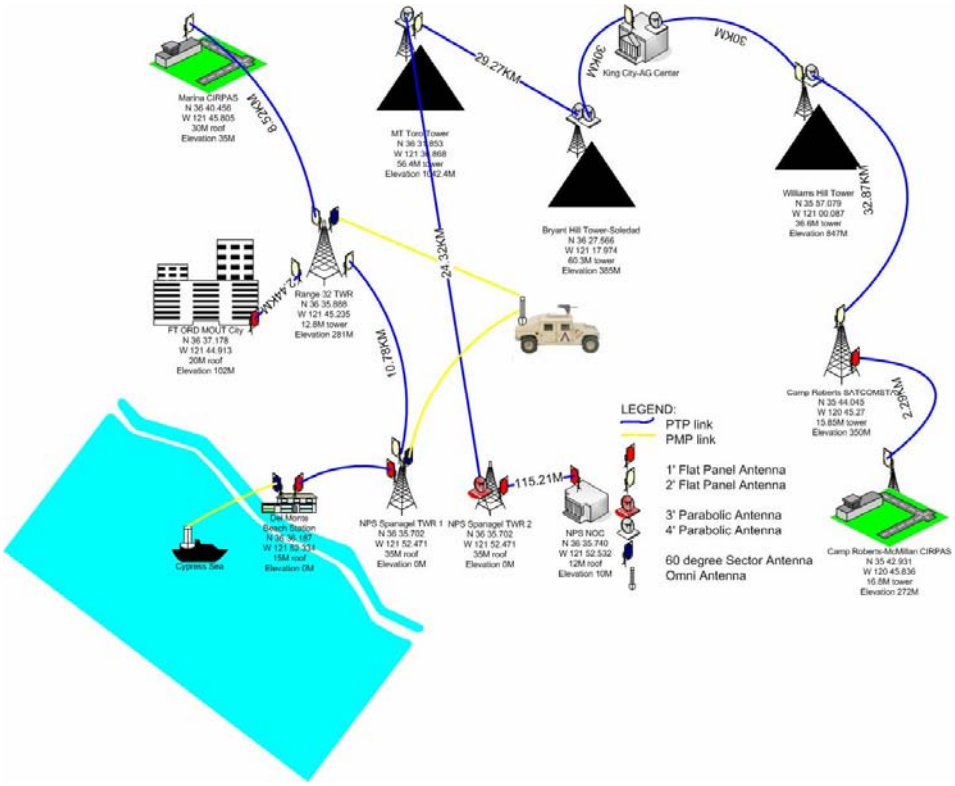


Figure 1. TNT Network Plan

This backbone connection of the network, along with connections to facilities at the beach laboratory in Monterey, the Center for Interdisciplinary Remotely Piloted

Aircraft Studies (CIRPAS) in Marina, California, Fort Hunter Liggett, the Military Operations in Urban Terrain (MOUT) facility at Fort Ord, U.S. Coast Guard facilities in San Francisco Bay, and Avon Park, Florida along with additional ground, air, and maritime locations, allows for a collaborative test-bed that provides a multi-theater C2 structure supporting missions and objectives of the CENETIX research team. The overall mission is to support advanced studies of wireless networking with unmanned aerial, underwater, and ground vehicles in order to provide flexible deployable network integration with an operating infrastructure for interdisciplinary studies of multiplatform tactical networks, Global Information Grid connectivity, collaborative technologies, situational awareness systems, multi-agent architectures, and management of sensor-unmanned vehicle-decision maker self-organizing environments.

The CENETIX testbed supports the following areas of research, where students and faculty alike can find their niche in testing and implementing the new concepts that will change the battlefield of the future. Specific areas of interest where students, staff and partners have participated:

- Adaptive wireless sensor-unmanned vehicle-decision maker networks.
- Ad hoc wireless mesh networks.
- Global Information Grid applications
- Network operations and Command Centers.
- Collaborative technology.
- Shared-situational and network awareness technology.
- Self-organizing network-centric environments.

- Multiple-agent intelligent systems.
- Satellite, ultra-wideband, and RFID communications.

C. CENETIX AND VPN SOLUTION

The future of the CENETIX Testbed will incorporate a Virtual Private Network (VPN) solution that will allow a global presence where multiple personnel and organizations can participate during future TNT experiments. These personnel and organizations include: Biometrics Fusion Center (BFC), Office of Force Transformation (OFT), Lawrence Livermore National Laboratory (LLNL), Defense Threat Reduction Agency (DTR), Coast Guard Station – Alameda (CGSA), as well as various allies both in the Continental U.S. and abroad where personnel in countries like Austria, Sweden, and Singapore have expressed a desire to participate.

These sites will incorporate either a hardware device (Cisco 3000 Series Concentrator), or a software solution (Cisco VPN Client) to perform reach-back capabilities to the Cenetix Testbed network located in the Network Operations Center onboard Naval Post Graduate School, Monterey, California.

The benefits of a VPN solution which will provide a secure means for all participants to be fully integrated in future TNT experiments will prove beneficial. The ability to collaborate amongst colleagues with various backgrounds and experiences will only serve to enhance these experiments.

THIS PAGE INTENTIONALLY LEFT BLANK

II. VPN OVERVIEW

A. WHY DO WE NEED A VPN SOLUTION?

In today's interconnected world, the need to move information from site to site is becoming common. Whether this move is from one end of town to the other or across the globe, the basic challenge is the same: How can we securely transport our data? For many years, this transportation was accomplished with expensive proprietary links that were leased from communication vendors so that companies had a "private" segment for such communications. The longer the distance, the more these connections costs, making wide area networks (WANs) a luxury that many firms could not afford. At the same time, many firms could not afford to go without them. As broadband Internet connections became staples for many firms, the concept of using the existing structure of the Internet as WAN cabling became an intriguing one. Costs could be greatly reduced using these already available public access points. The concern again was how to keep the data secure. Because we are sharing an international "party line" with anyone else who connects to the Internet, how can we be sure that our data is protected from eavesdropping, manipulation, un-authorized users, etc? The solution is Virtual Private Networking. (Zeltser, 161)

As we have seen VPNs were developed initially to deal with security issues of transmitting clear text data across a network. Clear text data is information that can be examined and understood by any person, including the source, destination, and anyone in between. Examples of applications that send traffic in a clear text format are

Telnet, file transfers via FTP, or TFTP, email using the Post Office Protocol (POP) or Simple Mail Transfer Protocol (SMTP), and many others. (Deal, 6)

Why do we need VPNs? There are a host of unethical individuals, such as hackers, who can take advantage of applications that send clear text data to execute the following type of attacks:

(1) Eavesdropping.

a. This is the most common type of attack with clear text.

b. A person examines the contents of packets as they are transmitted between two devices.

c. Both applications and protocols are susceptible to this type of attack, these include: Telnet, POP, HTTP, TFTP, FTP, SNMP.

i. Tools:

1. A protocol analyzer is used to sniff packets, on a PC with a promiscuous network interface card (NIC). The attacker must have access to a connection between the actual source and destination devices.

ii. Solution:

1. One way to overcome eavesdropping attacks is to use what e-Commerce company’s use, HTTP with SSL (HTTPS) to encrypt user-sensitive information.

2. Another solution is to incorporate a VPN solution with encryption. The encryption will scramble the clear text information into what would appear as a random string of characters; only the destination will be able to decipher the information. The following two methods are implemented in a VPN solution:

    a. Link Encryption – the entire frame is encrypted between point-to-point connections.

    b. Packet Payload Encryption – only the packet payload is encrypted, which allows Layer-3 network devices to route across the Internet. This is the most common encryption method you will see in VPN solutions, because of it’s scalability across multiple hops, only two devices need to handle the encryption/decryption process while the intermediate devices simply route the encrypted packets.

(2) Masquerading

a. This occurs when an individual hides their identity, possibly even assuming someone else's identity. This is accomplished by changing the source addressing information in packets. In the TCP/IP world this is commonly referred to as spoofing and typically associated with Denial of Service (DoS) and unauthorized access attacks.

i. Tools:

1. The attacker would use some sort of specialized packet-generating program which would allow him to specify the source address to be used, instead of using the IP address associated with the hacker's PC NIC.

2. This would allow the attacker to use an internal source address that a packet filter might allow, and then redirect that packet to through the firewall to his destination.

ii. Solution:

1. The most common solution is to use a packet integrity check system, which is implemented with a hashing function. Hashing functions allow you to

verify the source of transmitted packets. Because hashing functions use a one-way hash with a shared key, only the devices that have the key will be able to create and verify the hash values. With VPNs, the most common hashing functions used are MD5 and SHA.

(3) Man-in-the-Middle

a. This type of attack can take on many forms, of which there are two common attacks:

i. Session Replay

1. An attacker, sitting between two devices, captures the packets from the session. The attacker will then try to use the captured packets at a later time by replaying (resending) them.

2. The attacker’s goal is to gain access to the remote system with the same packets by changing the contents of the packets to assist in the process.

ii. Session Hijacking

1. An attacker will attempt to insert himself into an existing connection and then take over the connection between the two devices.

2. To execute this attack, the attacker will have to perform masquerading, where the attacker is pretending to be the source and destination devices. Plus, the attacker must have access to the packets flowing between the source and destination devices.

    a. Tools:

        i. Attackers will most commonly use an attack protocol analyzer to capture packets with the two types of attacks.

        ii. However with Session Replay attack, the hacker might use Java or Active X scripts to capture packets from a web server. And, with Session Hijacking attack, the attacker will need some type of specialized TCP sequence-number guessing program to successfully intercept and take over an existing TCP connection.

b. Solutions:

i. The most common way to solve these types of attacks would be to randomize the TCP sequence numbers, which would make it nearly impossible for the attacker to predict future sequence numbers for the session. This is possible due to the 32 bit length sequence number which has over 2 billion possible combinations.

ii. Another solution would be to incorporate a VPN solution. With VPNs three are utilized to combat man-in-the-middle attacks:

1. Device Authentication
2. Packet Integrity Checking
3. Encryption

B. WHAT IS A VPN?

The Internet possesses an unbelievable potential to facilitate e-commerce (both in the civil and military arena), however a few significant awkward impediments ought to be resolved in case an enterprise has to genuinely undertake real-time commercial activities across the Internet. The Internet's biggest advantages are its boundlessness and its universal availability. Yet these features are the medium's biggest vulnerability, as stated previously.

When researching what a VPN is and how it functions, you will arrive a multitude of definitions, functions, capabilities and proprietary terms. But, in the simplest terms a VPN is a connection that is established over an existing "public" or shared infrastructure using encryption and authentication technologies to secure its payload between two entities that are not necessarily directly connected. However, a good VPN solution will deal with most, if not all, of the following issues: (Deal, 12), (Zeltser, 161)

- Protecting data from eavesdropping by using encryption technologies such as RC-4, DES, 3DES, and AES.
- Protecting packets from tampering by using packet integrity and hashing function such as MD5 and SHA.
- Protecting against man-in-the-middle attacks by using identity authentication mechanisms, such as pre-shared keys or digital certificates.
- Protecting against replay attacks by using sequence numbers when transmitting protected data.

- Defining the mechanics of how data is encapsulated and protected, and how protected traffic is transmitted between devices.
- Defining what traffic actually needs to be protected.

C. HOW DOES IPSEC WORK?

IP Security, or IPsec, is a framework of standards that provides the following security features at the network layer between two peer devices:

- Data Confidentiality, Integrity, Authentication
- Anti-replay detection
- Peer authentication

With the CENETIX Lab the use of a device that provides network layer protection was at the forefront; protection of any IP traffic was required between peer devices, and IPsec provides that function. However, the downfall for implementing an IPsec VPN solution required the use of remote clients to install additional software in order to communicate with our VPN concentrator. This was accomplished by use of the Cisco VPN Client software, which is the same software students utilize for access to the NPS ERN wireless network.

IPSec is defined in Request for Comment (RFC) 2401, as well as being associated with a multitude of other protocols and standards as mentioned in other RFC's. However, the main functions that IPSec provides include: (Deal, 90)

- Data Confidentiality – accomplished via encryption to protect data from eavesdropping attacks, supported algorithms include DES, 3DES, and AES.
- Data Integrity and Authentication – accomplished via HMAC functions to verify packets have not been tampered with and are being received from a

valid peer; prevention of man—in-the-middle or session hijacking attacks. Supported functions include: MD5 and SHA-1.

- Anti-Replay detection - accomplished by use of sequence numbers in data packets to ensure that replay does not occur from a man-in-the-middle device.
- Peer Authentication – accomplished by use of symmetric or asymmetric pre-shared keys or digital certificates.

The two main groupings of standards that IPSec utilizes are:

- Internet Security Association Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE) – defined in RFC's 2407 and 2408 respectively, these standards are utilized to establish a secure management connection (Phase 1).

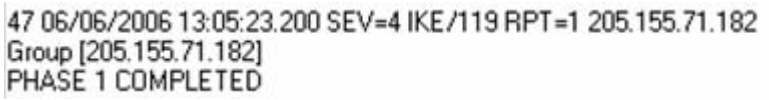


Figure 2. Phase 1 Completion – Series Manager

- Authentication Header protocol (AH) and Encapsulation Security Payload (ESP) – defined in RFC's 2402 and 2406 respectively, these standards are utilized to establish a secure data management connection (Phase 2).

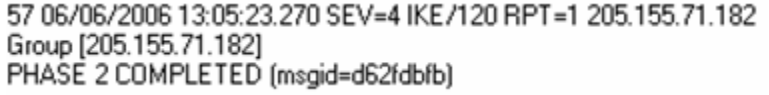


Figure 3. Phase 2 Completion – Series Manager

1. IPsec Connection Process

In the establishment of a secure IPsec connection, two peers will perform five basic steps. Once these processes are properly executed the secure connection will remain in

place until either a network failure occurs or either one of the peers terminates the link. A brief description of the processes is as follows:

(1) The IPsec process is triggered by a pre-configured station (either remote, or local).

(2) IPsec will initiate an ISAKMP/IKE Phase 1 (management connection); no data is being transversed.

a. Phase 1 is responsible for setting up the secure management connection, either in the main or aggressive mode.

b. During the Phase 1 process you would find the encryption processes (DES, 3DES, AES) are being validated, the HMAC function (MD5, SHA-1) are implemented, and the pre-shared keys are verified.

c. Uses UDP port 500; this is important if utilizing a firewall. If administrators fail to establish port 500 access, problems will occur when utilizing Network Address Translation – Transversal (NAT-T) over port 4500.

(3) IPSec will negotiate the defined security parameters (data transform set), and confirm them in order to build a secure data connection (Phase 2).

a. Phase 2 is responsible for establishing and enforcing the security protocols and transform for the connection.

b. IPsec can use two security protocols to protect the data transmitted over the connections that are being built. They are Authentication Header (AH) and Encapsulation Security Payload (ESP), defined in RFC 2402 and 2406 respectively.

c. A data transform set contains: the security protocol (AH and/or ESP, connection mode (tunnel or transport), encryption information (DES, 3DES, AES-128/192/256), packet authentication and verification (MD5, or SHA-1).

i. These transforms are commonly referred to as a Security Association (SA) in which all of the necessary security components to communicate successfully with an IPsec peer are defined.

(4) HMAC functions will be initiated and devices will begin to share user data securely.

(5) Connection is properly made, data is transversed; the management and data connections will remain in place until administrative requirements are reached (lifetime limits, network and user requirements).

2. IPsec and Firewalls

There are two basic ways VPN traffic is terminated in networks: on a firewall, or a device that is behind a firewall. In order to properly configure a IPsec tunnel through a firewall, the following needs to be configured on the device that is providing perimeter security.

As we experienced in the Coast Guard Station – Alameda location, the following configurations are required for firewall devices (Deal 126-127):

- Management Connections: UDP port 500
- Data Connections using AH: protocol 51
- Data Connections using ESP with no NAT-T: protocol 50
- Data Connections using ESP with NAT-T: UDP port 4500
- Data Connections using ESP with IPsec over UDP: UDP port 10000 (default setting, but can be changed)
- Data Connections using ESP with IPsec over TCP: TCP port 10000 (default setting, but can be changed)
- During pre-test configurations which simulated the CGSA equipment string, the following figure indicates the final settings for my router. From my home, I was able to construct a circuit which provided a NAT-T VPN tunnel to the ***tnt06vpn*** concentrator located on NPS.

D. WHAT DEVICE DID WE USE TO ESTABLISH A VPN?

There are many options to implement a VPN solution, such as a PIX or ASA router, The Cisco VPN 3000 Series Concentrator offers the best-in-class remote-access VPN device that provide businesses with unprecedented cost savings through flexible, reliable, and high-performance remote-access solutions. Cisco acquired Altiga, which initially built the VPN hardware appliances in 2000, and have developed the VPN 3000 Series concentrators to provide solutions for the most diverse remote-access deployments by offering both IP Security (IPSec) and Secure Sockets Layer (SSL)-based VPN connectivity on a single platform.

There are six different classes of the Cisco 3000 Series concentrators, use of the 3005 and 3015 were preferred for use in the CENETIX Lab. The following table depicts a comparative of all six models.

	Cisco VPN 3005	Cisco VPN 3015	Cisco VPN 3020	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Simultaneous IPSec Remote Access Users[1]	200	100	750	1,500	5,000	10,000
Simultaneous WebVPN (Clientless) Users[2]	50	75	200	500	500	500
Maximum LAN-to-LAN Sessions	100	100	250	500	1,000	1,000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	SW	SW	HW	HW	HW	HW
Available Expansion Slots	0	4	1	3	2	0
Encryption (SEP) Module	0	0	1	1	2	4
Redundant SEP	-	-	Option	Option	Option	Yes
System Memory	32/64 MB (fixed)	128 MB	256 MB	128/256 MB	256/512 MB	256/512 MB
Hardware Configuration	1U	Scalable 2U	Fixed 2U	Scalable 2U	Scalable 2U	Fixed 2U
Dual Power Supply	Single	Option	Option	Option	Option	Yes
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

Table 1. 3000 Series Concentrator Comparison (From: Deal, 182)

As you can see, the Cisco 3000 Series concentrators are a robust piece of equipment, however depending upon your VPN solution and the capabilities that you desire the Concentrator is not the only solution.

Cisco has three platforms choices for L2L sessions: Concentrators, Routers, and Private Internet Exchange (PIX) and Adaptive Security Algorithm (ASA) security appliances. Although the Concentrator does not possess the same capabilities of the other devices listed (limited routing

functions, limited QoS support, and limited address translation to name a few), it's main advantage which is why we utilize this device in the CENETIX Lab is it's simplicity in configuring L2L sessions. Furthermore, due to the size (rather small) of the CENETIX Testbed Network a concentrator is ideal in that it is not complicated to administer.

The product of choice for the CENETIX Lab is the Cisco 3015 VPN Concentrator, see figure below. When comparing the other models available, the 3015 provided the most favorable solution in scalability, system memory, and the amount of clientless remote user access. (Table 1)

Figure 4. Cisco 3015 VPN Concentrator

E. WHERE WE INSTALLED VPN DEVICES?

The reach of the TNT Experiments extends beyond the Naval Post Graduate grounds is essential to fully integrate, not only the primary agent (SOCOM) but those organizations throughout the United States as well, with future plans to extend L2L VPN tunnels with allied forces in both the European and Asia-Pacific theaters. During TNT

06-2 the primary participants included: the Biometrics Fusion Center (BFC), Lawrence Livermore National Laboratory (LLNL), the Department of Forestry (Missoula), Special Ops Command (Avon Park), Northern Command (Northcom), and Coast Guard Station Alameda (CGSA). CENETIX Lab was able to purchase 3 Cisco VPN 3015 Concentrators prior to the start of TNT 06-2, and a vast amount of coordination with NPS ITACS and the above organizations was accomplished before commencement of TNT 06-2, on 1-Mar-2006. The organizations where the Cisco 3015 Concentrator (3015) was installed included: BFC, Avon Park, and attempts were made unsuccessfully to install at the CGSA.

Some distant stations did not receive a VPN Concentrator; however they were assigned VPN Client accounts for access to the TNT network, and afforded the same privileges of a IPsec connection. The Cisco VPN Client is a VPN remote access client that runs on Microsoft Windows PC, Linux PCs (Intel based), Macintoshes (MAC OS X), and Sun UltraSPARC workstations (Solaris). For both the Windows and Macintosh environments, a graphical user interface (GUI) is utilized and represented in the following figure.

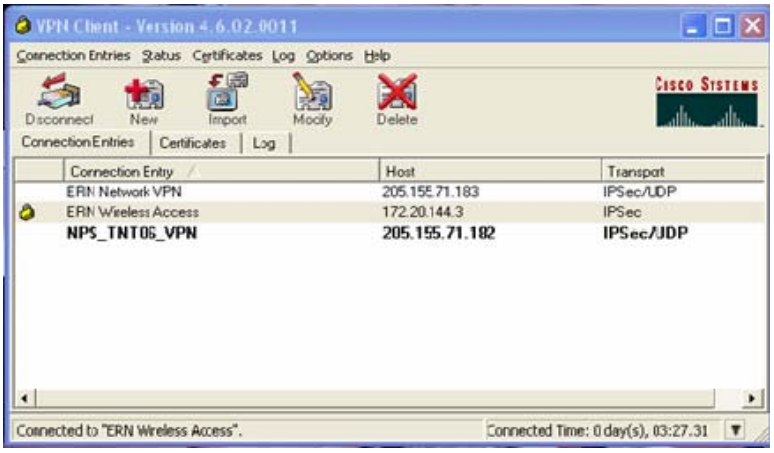


Figure 5. VPN Client

F. ADVANTAGES/DISADVANTAGES OF VPN

Some of the questions that must be considered and answered when contemplating a VPN solution include:

- What is the confidence level of the data you are sending?
- What do I need to protect?
- What kind of protection is required?
- What value is placed on the secrecy?
- How important is it to know the source of received data?
- Is it scalable?
- What is the cost?

These questions are only represent a very few that could be asked. However, they are some of the more important questions that need to be addressed up front. First off consider the two alternatives to a VPN solution, dedicated lines and the unencrypted Internet. With the first alternative, the high cost of a dedicated T1 line would be futile in today's realm. The cost of operating and maintaining a T1 is like renting a home when you could buy a house. The Internet today is robust enough to handle most organizational bandwidth requirements. The problem is how the organizations utilize the Internet to its utmost, while providing protection to their interest.

To leverage the functionality of the Internet and increase the security level of communications, a VPN solution is ideal. The encryption would protect the data; however it would add a slight burden to the organizations network and possibly decrease the bandwidth to a small degree. As with most IT solutions, encryption comes at a price. The more encryption you require, the more cost you are going to incur.

The major advantages of a VPN include: Security, Deployment Advantages, and Cost Effectiveness. With security the three most basic IT requirements are considered and implemented in a VPN solution. First, confidentiality, to guarantee that no unauthorized personnel are going to be able to view your information or that the algorithms utilized scramble the private data from viewing are the most important aspects of VPNs. Second, data integrity, verification of information that is received and comparison of that information with hashes or digital signatures provides a level of protection through encryption and VPN use. Last, authentication, verification that the information came from whom it was suppose to, and also verifying whoever received that information was authorized to receive it.

Concerning the deployment advantages and cost effectiveness of a VPN solution, both the economic advantages and ease in utilizing existing infrastructure in the installation of a VPN would be evident once the project was initiated. Because VPNs can utilize existing infrastructures, the need to install new cable for connectivity is minimal. This in turn would save in installation, operation and maintenance costs. Furthermore, VPNs would replace the need for organizations to rely heavily upon high-cost, dedicated WAN links. As well as remote users, who most probably have broadband connectivity at their disposal, would no longer be required to utilize a dedicated dial-in phone line. Regardless of the network setup, in most cases a VPN can give an organization an excellent return on investment and add up considerable savings in the long run. (Zeltser, 167-168)

The major disadvantages of a VPN include: Processing Overhead, Packet Overhead, Implementation Issues, Troubleshooting and Control Issues, and Internet Availability Issues. Although VPNs provide a significant amount of advantages to an organization, there are some disadvantages that should be carefully considered when pushing a VPN solution. The amount of overhead from the additional packets that are transported, as well as the additional load on systems and devices in the network performing encryption, will degrade the performance of the network over time. Two problems experienced during TNT 06-2 and 06-3 involved troubleshooting and Internet availability issues. Due to the CENETIX Lab being operated solely by students and professors, NPS ITACS was hesitant to allow full control on the devices that students required administrative access during preparations for TNT 06-2. During 06-3 in conjunction with CGSA, constructing Internet access as well as a secure tunnel to the TNT network was challenging. However, with utilizing the functions inherent to the Cisco 3015 Concentrator, and NAT-T, a solution was constructed.

THIS PAGE INTENTIONALLY LEFT BLANK

III. OBSERVED EXPERIMENTS

A. TNT 06-2

Prior to TNT 06-2, only one VPN tunnel was established in previous experiments, to the BFC. The initial configuration, Fig-6, was established during TNT 06-1, and proved the concept of a VPN solution and the ability for external organizations to reach-back into the TNT Network. Expanding on these findings, extending the VPN architecture to more organizations via a L2L IPSec tunnel was planned for and installed prior to TNT 06-2 (Fig-7).

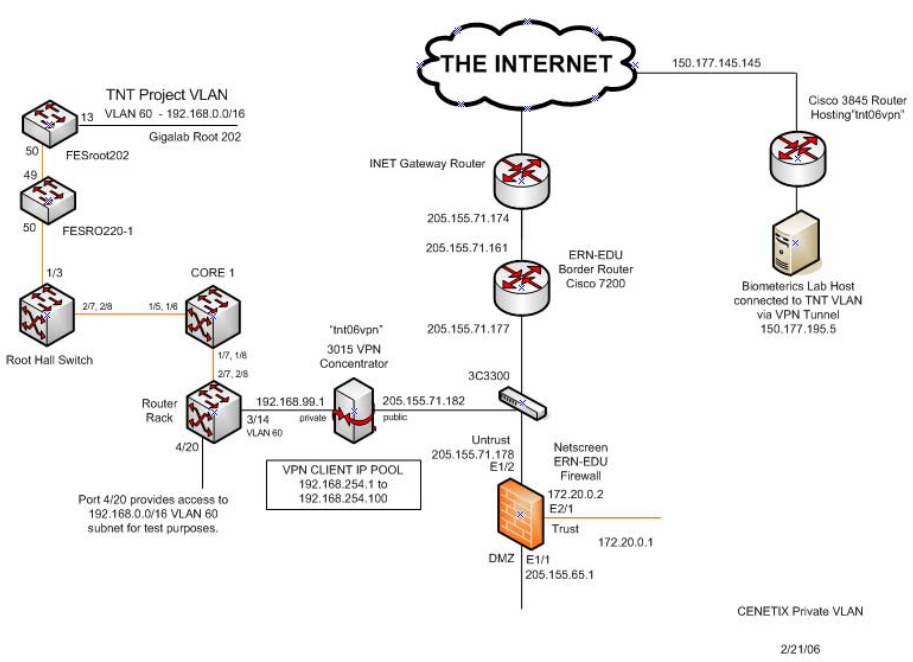


Figure 6. TNT Architecture prior to TNT 06-2.

In preparation for the TNT 06-2 Experiment, coordination with Mike Williams at the Information Technology Assistance Center (ITAC) was crucial. Because, CENETIX Lab personnel are predominantly comprised of students, administrative privileges to make network changes is difficult and when required, the requests for changes

are at best second fiddle to normal day-to-day NPS NOC operations. However, the assistance and patience of Mike Williams, in assisting the CENETIX Lab with network changes was nearly completed prior to commencement of the experiment on 27Feb06. Prior to the start of TNT 06-2, a majority of my time dealt with learning about VPN technology, coordination with participating organizations, and configuration of the TNT and Avon Park Concentrators.

The VPN architecture, after the installation of two 3000 Series VPN Concentrators at the MSC and Avon Park, while coordinating with the BFC in the configuration of a Cisco 3845 router, the TNT 06-2 architecture shown in the below figure was designed:

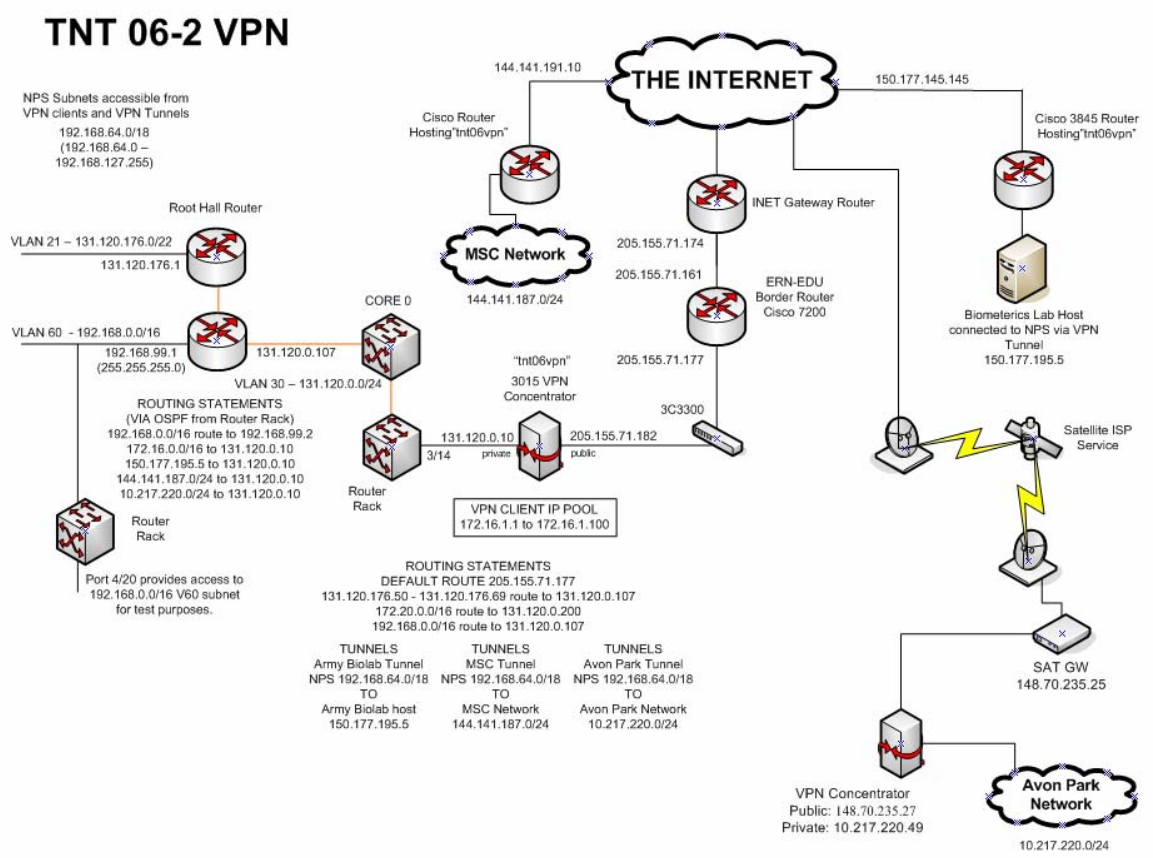


Figure 7. TNT Architecture TNT 06-2.

The number of participants who required VPN access to the 06-2 experiment included: The Biometrics Fusion Center – West Virginia, Special Operations Command – Avon Park, Naval Special Warfare Group One (Mission Support Center) – Coronado, and Coast Guard Station – Alameda. These locations were configured using the Cisco 3005 and 3015 VPN Concentrators with the exception of the BFC who utilized a Cisco 3845 Router (vice the 3015 that was provided and successfully implemented during TNT 06-1).

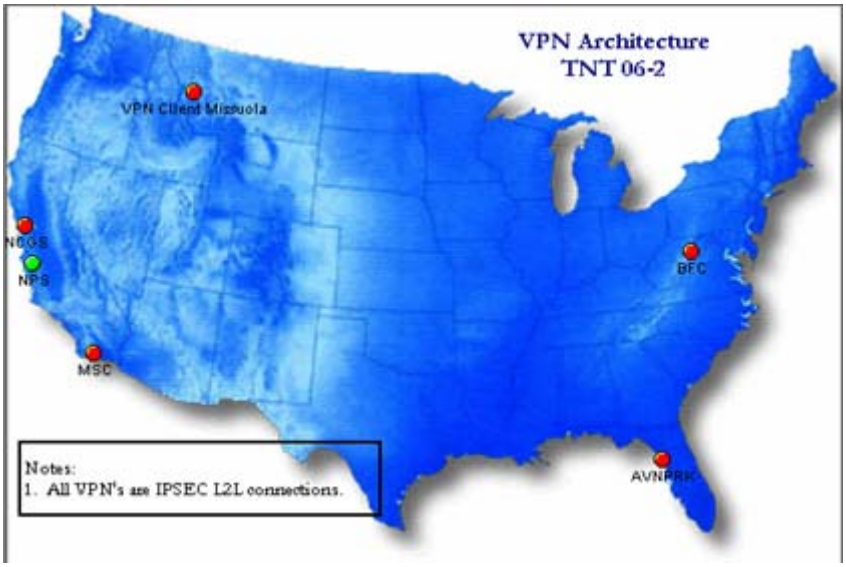


Figure 8. VPN Nodes TNT 06-2 (CONUS).

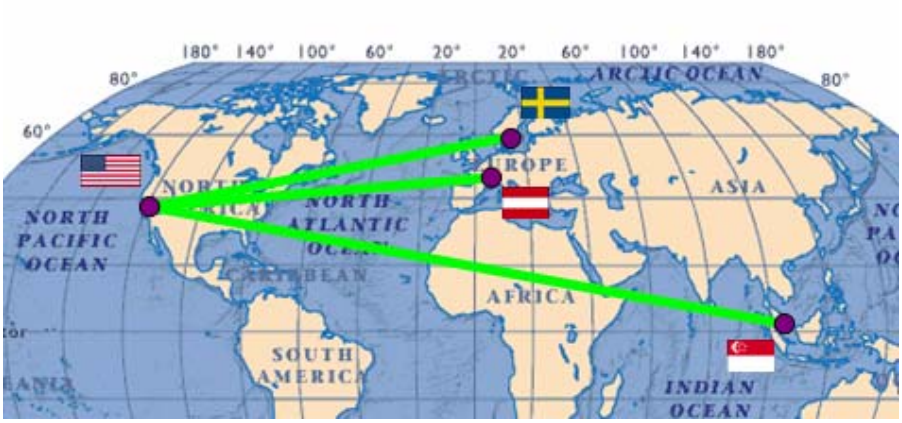


Figure 9. VPN Nodes TNT 06-2 (OCONUS).

Other organizations (Figs. 7 and 8) who did not have the necessary equipment to establish a VPN circuit via hardware were provided user accounts in order that they could log-in and participant on the nps_tnt_vpn06 network. Again coordinating with Mike Williams at ITAC, we created the following accounts (and passwords) for users to log-in using the Cisco VPN Client software. Planned users included:

One – Biometrics Fusion Center
Two – Lawrence Livermore National Laboratory
Two – Dept of Forestry – Missoula, MT
Six – Special Ops Command – Avon Park
Two – Northcom – Colorado
Two – Sweden
Two – Austria
Two - Singapore

Once the VPN Client accounts were created, they were provided the information by means of digitally signed, encrypted messages with the necessary information to log-in on the nps_tnt_vpn06 network via a secure tunnel. The below screen depicts what the users would have seen once they loaded the Cisco VPN Client Software and the necessary nps_tnt06_vpn profile on their systems.

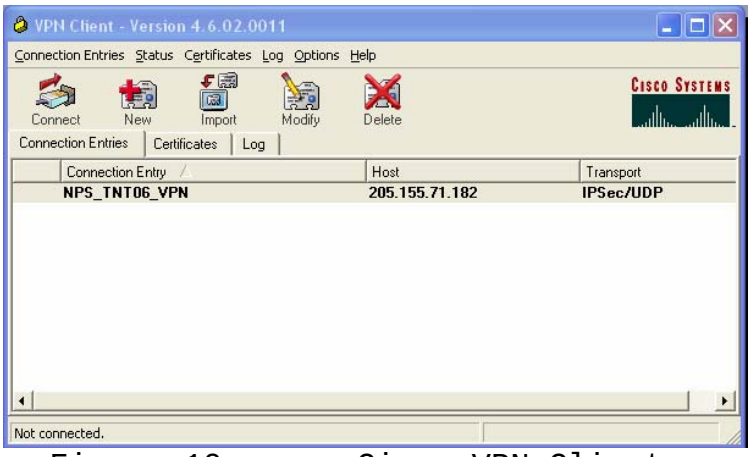


Figure 10. Cisco VPN Client.

1. Configuring the VPN Concentrator

a. Configuration

With VPN 3015s, three Ethernet interfaces are available, and with the VPN 3005 only two Ethernet interfaces are available. When configuring the nps_tnt06_vpn, located in ITACS, only two interfaces were utilized. Ethernet 1 pointing toward inbound private traffic (internal LAN), 131.120.0.10 and Ethernet 2 pointing to outbound public traffic, 205.155.71.182. When configuring the interfaces, you must configure the two interfaces that physically connect your network.

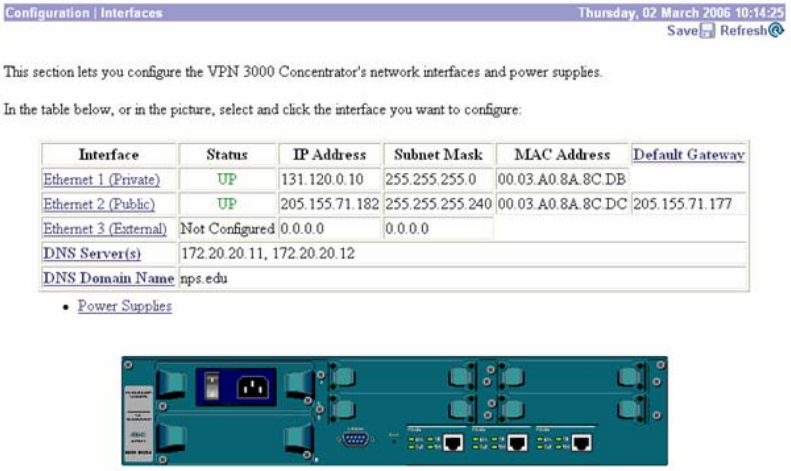


Figure 11. Cisco 3015 Interfaces TNT 06-2.

(1) Configuring Ethernet 1. When configuring Ethernet ports only one port can be checked as Public Interface. As in the case of Ethernet 1, it is not checked as public, due to the private IP Adx of 131.120.0.10.

Since the public box is not checked, this makes Ethernet 1 Private, the default setting for this interface. With Private setting all packets except source-routed IP packets are allowed.

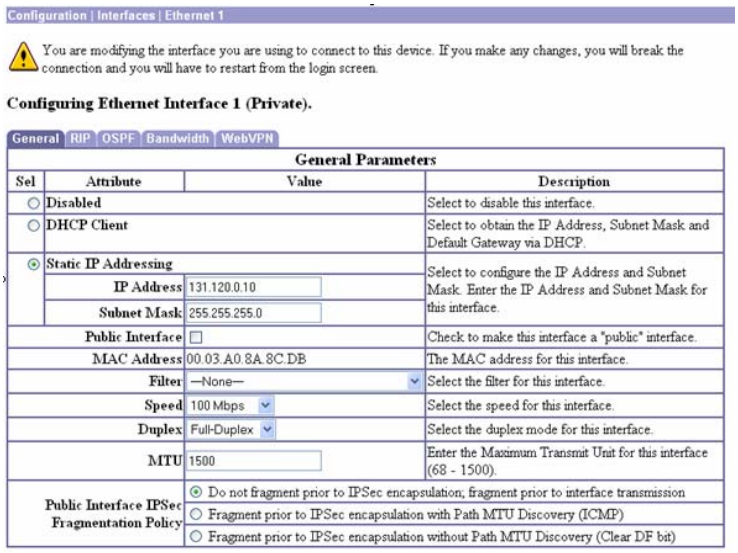


Figure 12. Interface Configuration Ethernet1.

(2) Configuring Ethernet 2. Interface is set to Public – Allows inbound and outbound tunneling protocols plus ICMP and VRRP, fragmented IP packets, and drops everything else, including source-routed packets.

The distant stations (BFC, AvnPrk, and MSC) would need to ensure that 205.155.71.182 is configured on their systems as the public interface; otherwise the L2L connection will fail with our 3015.

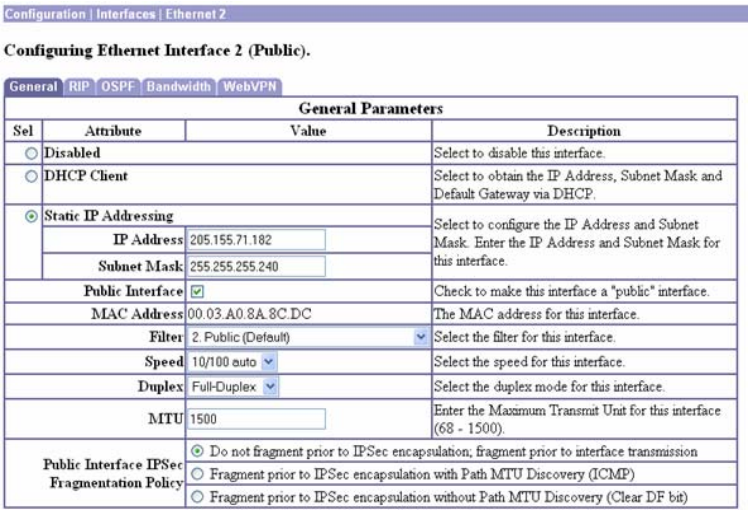


Figure 13. Interface Configuration Ethernet2.

(3) System Information. Entering the VPN system information, such as, name and time will assist in future troubleshooting of this circuit. For CENETIX VPN circuit, the assigned name is: ***tnt06vpn***.

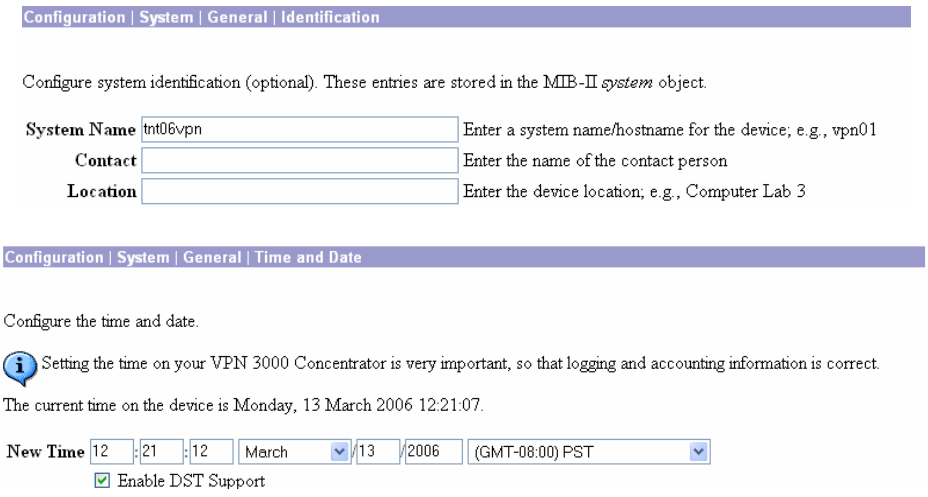


Figure 14. Cisco 3015 General Configuration.

(4) Configuring Tunneling Protocols. The nps_tnt06_vpn is configured using IPsec, L2L. When initiating a site-to-site session VPN seven steps are performed in the establishment of a secure session. The following steps are as follows:

- One VPN gateway peer initiates a session to the remote VPN gateway peer.
- ISAKMP/IKE Phase 1 begins when the peers negotiate how the management connection will be protected.
- ISAMP/IKE.
- RFC 2407 - Internet Security Association and Key Management Protocol (ISAKMP) defines how devices communicate with each other via IPsec, defines the different kinds of communications and acknowledgements (responses), and how IPsec communications are packaged into an understandable format.
- ISAKMP is a generic key management and security association creation protocol for use in TCP/IP networks.
- RFC 2409 – Internet Key Exchange (IKE) protocol is a hybrid protocol which is responsible for negotiating, creating, and refreshing keying information to protect IPsec connections. Where IKAMP defines the framework, IKE defines the mechanics on how the process of dealing with keying material accomplished.
- IKE is an implementation of ISAKMP used for IPSEC key management.
- Diffie-Hellman is used to share the keys securely for encryption algorithms and HMAC functions of the management connection.
- Diffie-Hellman Key Exchange addresses this problem and Internet Key Exchange (IKE) uses this Diffie-Hellman to ensure that a shared key can be generated and shared across a public connection in a way that is infeasible for anyone to work out the key. This shared key can then be used with an encryption algorithm such as DES, 3DES, IDEA etc.
- RFC 2104 - Hashing Message Authentication Codes (HMAC) a subset of hashing functions that specifically address the authentication issues with data and packets. HMACs are a shared secret symmetric key to create the fixed output, called a digital signature or fingerprint.

- Symmetric Key – use single key to provide a security function to protect information. This form of keying is very efficient and fast, and typically used for encryption and packet integrity checking. Typical forms of keying that utilize symmetric keying: DES, 3DES, AES. Types of hashing functions that use symmetric keying: MD5 and SHA.
- Device authentication is performed across the secure management connection.
- ISAKMP/IKE Phase 1 ends and Phase 2 begins: the peers negotiate the parameters and the keying information to protect the data connections (this is done across the secure management connection or, optionally by using Diffie-Hellman again).
- The data connections are established and Phase 2 ends: the VPN gateways can now protect user traffic across the data connections.
- Management and data connections will remain active until they expire, and must be rebuilt.

Capitalizing on the security features that IPsec utilizes, as well as the security policies that are in place at the distant stations (BFC, AvnPrk, MSC) who desire to participate in the TNT experiments. It was determined that L2L IPsec tunnels provide the best solution for the CENETIX testbed to implement. The figure below shows the three L2L Sites that were installed, configured, and operated during TNT 06-2. Configuration of these three circuits required a significant amount of my time in coordination with network personnel both here at the NPS ITACS NOC, and the distant station NOCs. Although challenging, this situation presented the management piece of my thesis research.

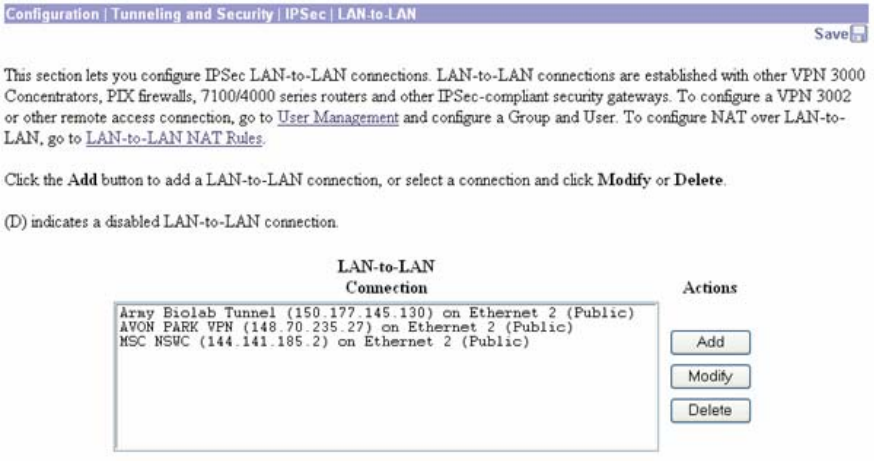


Figure 15. IPsec L2L Connections TNT 06-2.

(5) Biometrics Fusion Center (BFC). The expertise at the BFC is utilized in the analysis of data files that the detection teams have gathered. Collaboration of users is conducted via the Groove peer-to-peer tool.

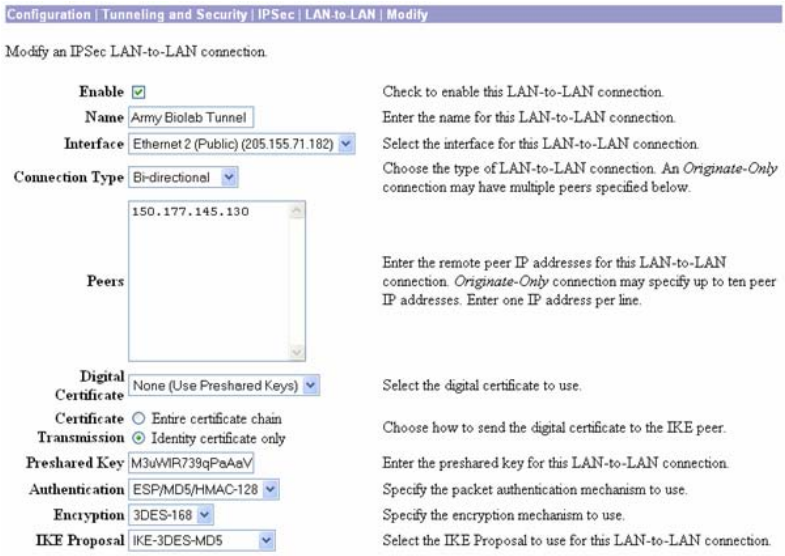


Figure 16. IPsec L2L Config TNT 06-2 (BFC)

(6) Avon Park. As a major contributor to the efforts of TNT/CENETIX, the ability to observe the experiments in the field allows SOCOM to participate.

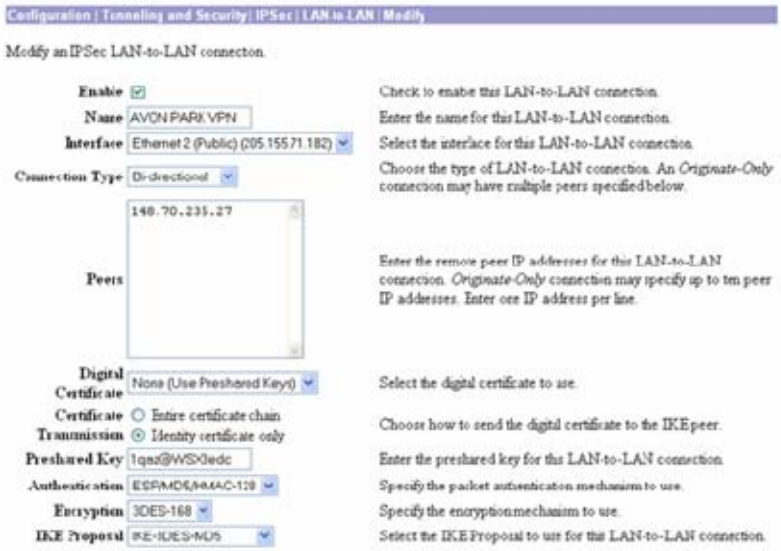


Figure 17. IPsec L2L Config TNT 06-2 (Avon Park)

(7) MSC NSWC. As a major contributor to the efforts of TNT/CENETIX, the ability to observe the experiments in the field allows Naval Special Warfare Command to participate.

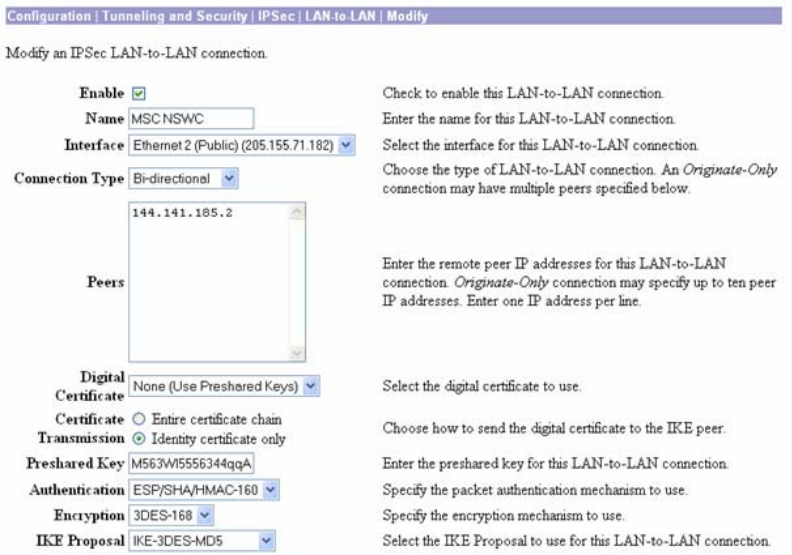


Figure 18. IPsec L2L Config TNT 06-2 (MSC).

b. Observations

Initially observations for both Camp Roberts and Coast Guard station Alameda were going to be monitored by

use of SolarWinds and the VPN 3000 Concentrator Series Manager. However, we could not meet the requirements for this experiment to install a dedicated line for the VPN connection to CGSA during TNT -6-2.

With the VPN 3000 Concentrator Series Manager multiple views and the ability to make changes via a web-enabled interface is possible. Because CENETIX Lab is operated by students and faculty, a GUI interface is ideal for the management of the VPN device. This proved vital for our observations; until SNMP was enabled then we could start using SolarWinds to monitor the VPN status, on a limited scale.

By typing in the nps_tnt06_vpn Concentrator IP Adx of 131.120.0.10, we were authorized minimal privileges to view the system configuration and monitoring tools. This access is granted from those administrators who are authorized to add users and grant privileges. Authorized users can then access the VPN 3000 Series Manager via a HTTPS (preferred) or HTTP (which will then ask if you would like to install SSL certificate) connection from a web browser. During my observations both Internet Explorer 6.0 and Mozilla Firefox 1.5.0.6 browsers were utilized without any problems.

Figure 19. Cisco 3015 Log-In Screen

This Series Manager allows many valuable quick observation tools for the network administrator to remotely (or locally) view the VPN Concentrator, and make quick adjustments to the configuration if necessary. This tool was predominantly used during TNT 06-2 and 06-3, and allowed easy management of L2L sites as well as remote user account management. Furthermore, this tool provided a means for monitoring the log files which provided valuable insight during troubleshooting. The figure below is the initial screen which allows management of three main areas of operations: Configuration, Administration, and Monitoring.

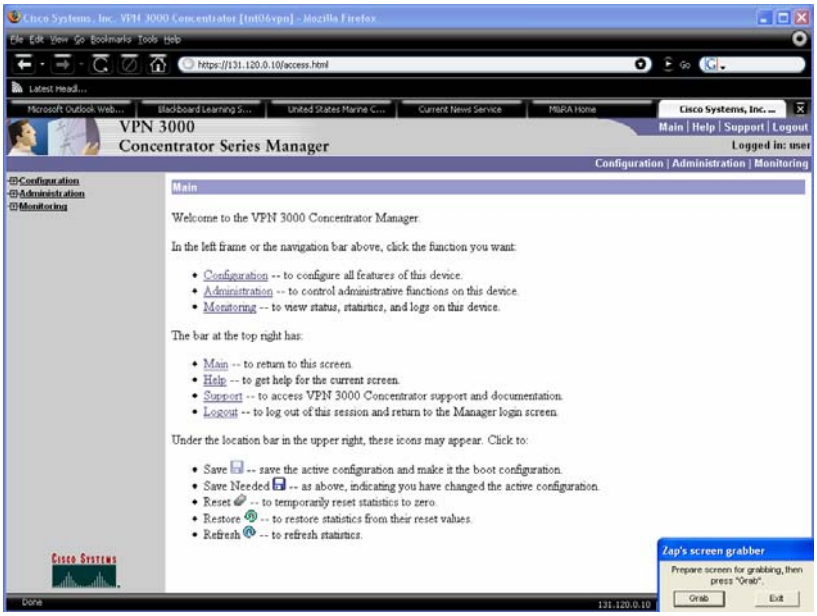


Figure 20. Cisco 3015 Concentrator Manager

The Top 10 Lists provide the following data for Network Managers to evaluate performance (shows statistics for the top 10 currently active VPN Concentrator sessions) sorted by data, duration and throughput. Administrators would find the session transmitting the most data, and the session that has been connected the longest to be the most useful information. The figures below represent the actual data collected during TNT 06-2:

(1) Data. Represents the amount of data transmitted since the user connected, this is not an average rate, which unlike SolarWinds can be determined (Fig-37).

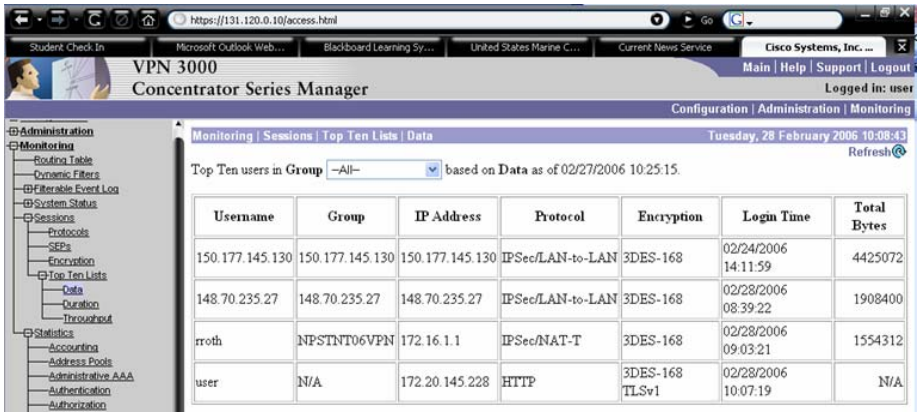


Figure 21. Series Manager Top Ten (Data)

(2) Duration. The amount of time a session has been active.

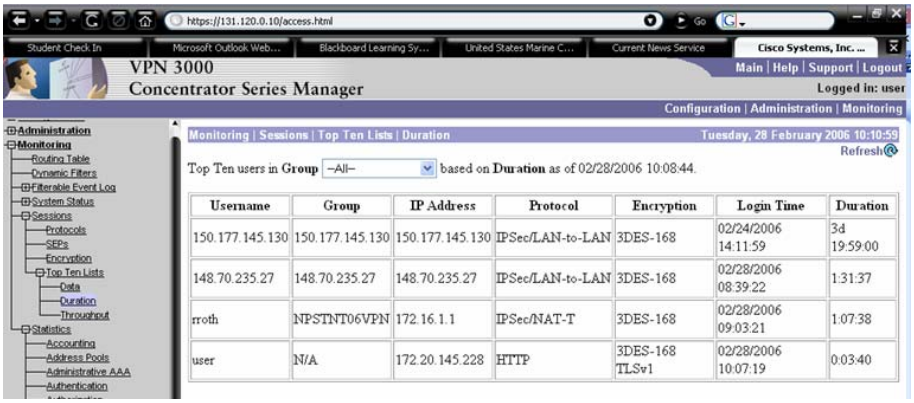


Figure 22. Series Manager Top Ten (Duration)

(3) Throughput. The average throughput could be used in determining who is consuming the most bandwidth.

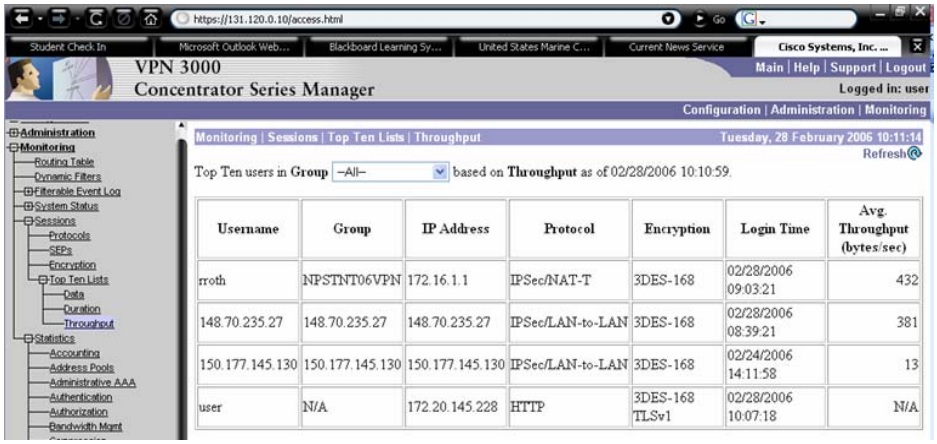


Figure 23. Series Manager Top Ten (Throughput)

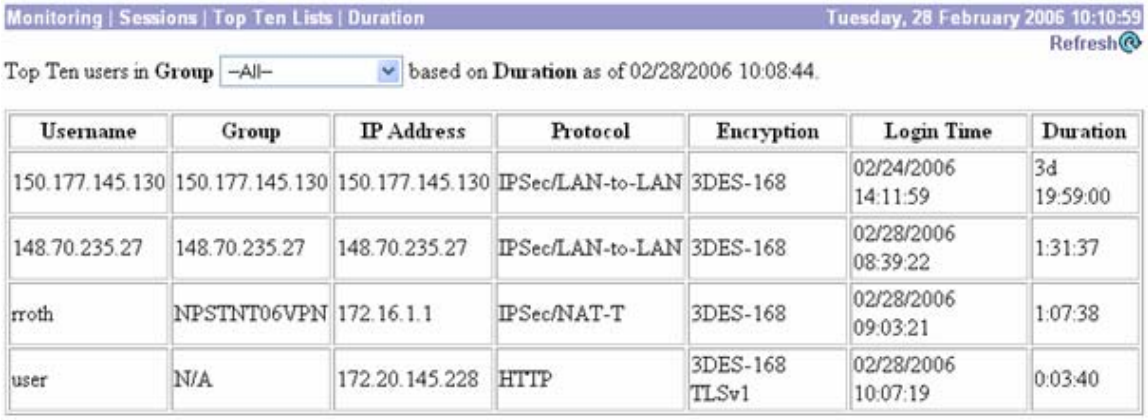
(4) Final Checks, 28-Feb-06. During the final installations and configurations for TNT 06-2, both the BFC (150.177.145.130) and Avon Park (148.70.235.27) connections initiated a successful session. However, the MSC connection failed due to firewall settings at Coronado Network Operations Center. Coordination between the MSC and their immediate NOC was occurring during this time, and success was not achieved until late afternoon on 28Feb06 (Fig-29). The main problem that impeded MSC from successfully establishing a L2L IPsec VPN tunnel was that the Access Control Lists (ACLs) were not allowing IPSec traffic to tunnel through.

Monitoring | Sessions | Top Ten Lists | Data
Tuesday, 28 February 2006 10:08:43
Refresh

Top Ten users in **Group** –All– based on **Data** as of 02/27/2006 10:25:15.

Username	Group	IP Address	Protocol	Encryption	Login Time	Total Bytes
150.177.145.130	150.177.145.130	150.177.145.130	IPSec/LAN-to-LAN	3DES-168	02/24/2006 14:11:59	4425072
148.70.235.27	148.70.235.27	148.70.235.27	IPSec/LAN-to-LAN	3DES-168	02/28/2006 08:39:22	1908400
rroth	NPSTNT06VPN	172.16.1.1	IPSec/NAT-T	3DES-168	02/28/2006 09:03:21	1554312
user	N/A	172.20.145.228	HTTP	3DES-168 TLSv1	02/28/2006 10:07:19	N/A

Figure 24. TNT 06-2 Pre-Check (Data)



Monitoring | Sessions | Top Ten Lists | Duration — Tuesday, 28 February 2006 10:10:59

Refresh

Top Ten users in **Group** –All– based on **Duration** as of 02/28/2006 10:08:44.

Username	Group	IP Address	Protocol	Encryption	Login Time	Duration
150.177.145.130	150.177.145.130	150.177.145.130	IPSec/LAN-to-LAN	3DES-168	02/24/2006 14:11:59	3d 19:59:00
148.70.235.27	148.70.235.27	148.70.235.27	IPSec/LAN-to-LAN	3DES-168	02/28/2006 08:39:22	1:31:37
rroth	NPSTNT06VPN	172.16.1.1	IPSec/NAT-T	3DES-168	02/28/2006 09:03:21	1:07:38
user	N/A	172.20.145.228	HTTP	3DES-168 TLSv1	02/28/2006 10:07:19	0:03:40

Figure 25. TNT 06-2 Pre-Check (Duration)

Monitoring | Sessions | Top Ten Lists | Throughput — Tuesday, 28 February 2006 10:11:14

Refresh

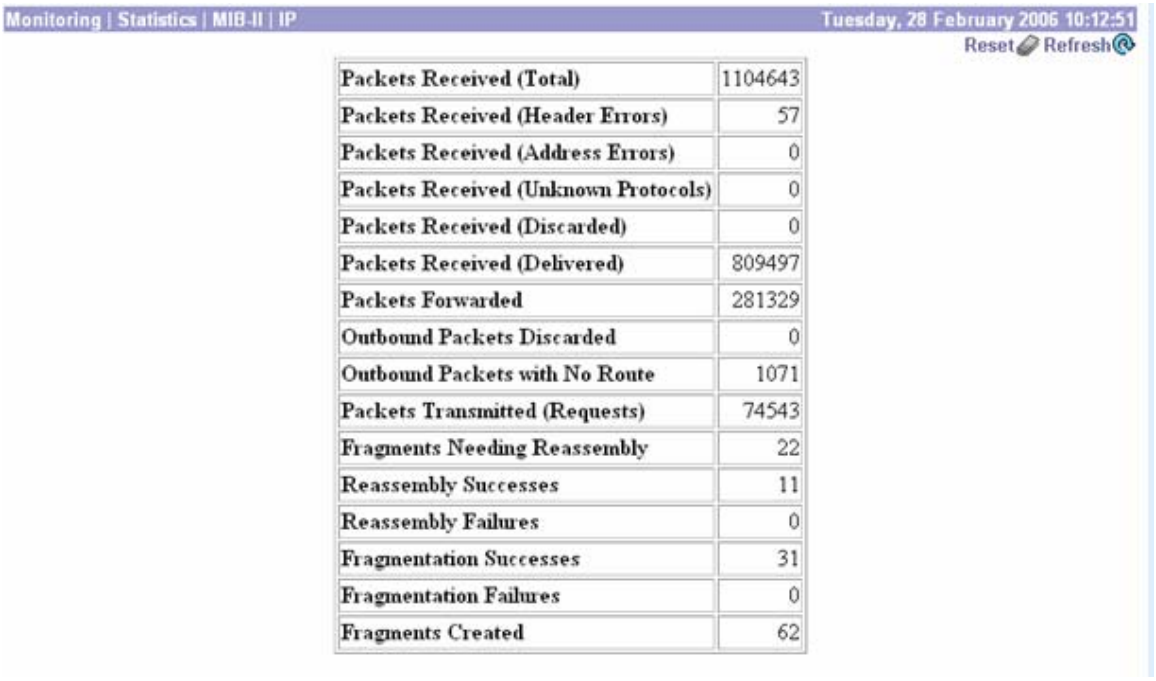
Top Ten users in **Group** –All– based on **Throughput** as of 02/28/2006 10:10:59.

Username	Group	IP Address	Protocol	Encryption	Login Time	Avg. Throughput (bytes/sec)
rroth	NPSTNT06VPN	172.16.1.1	IPSec/NAT-T	3DES-168	02/28/2006 09:03:21	432
148.70.235.27	148.70.235.27	148.70.235.27	IPSec/LAN-to-LAN	3DES-168	02/28/2006 08:39:21	381
150.177.145.130	150.177.145.130	150.177.145.130	IPSec/LAN-to-LAN	3DES-168	02/24/2006 14:11:58	13
user	N/A	172.20.145.228	HTTP	3DES-168 TLSv1	02/28/2006 10:07:18	N/A

Figure 26. TNT 06-2 Pre-Check (Throughput)

This section of the Manager lets you view statistics that are recorded in standard MIB-II objects on the VPN Concentrator. MIB-II (Management Information Base, version 2) objects are variables that contain data about the system. They are defined as part of the Simple Network Management Protocol (SNMP); and SNMP-based network management systems can query the VPN Concentrator to gather the data. However, the 3000 Series Manager can not “walk” the hierarchical MIB tree; a few of the VPN MIB-II variables were walked by using SolarWinds, once SNMP was enabled (see Fig-43, 44). One statistic of interest for my

observations is shown in Fig-25; this screen shows the statistics of the MIB-II objects for IP traffic on the VPN Concentrator since it was last booted or reset, prior to 28Feb06. For a more specific IP MIB object definition refer to RFC 2011. The Series Manager allows for monitoring of up to nine different objects. The items of interest include: Packets Received (Total), Packets Received (Discarded), Packets Received (Delivered), Packets Forwarded, Outbound Packets with No Route, Packets Transmitted (Requests), Fragments Needing Reassembly, Reassembly Successes, Fragmentation Successes, Fragments Created. These items are discussed in more detail below. (CP-II, 226-227)



Packets Received (Total)	1104643
Packets Received (Header Errors)	57
Packets Received (Address Errors)	0
Packets Received (Unknown Protocols)	0
Packets Received (Discarded)	0
Packets Received (Delivered)	809497
Packets Forwarded	281329
Outbound Packets Discarded	0
Outbound Packets with No Route	1071
Packets Transmitted (Requests)	74543
Fragments Needing Reassembly	22
Reassembly Successes	11
Reassembly Failures	0
Fragmentation Successes	31
Fragmentation Failures	0
Fragments Created	62

Figure 27. Series Manager MIB-II IP Stats

Packets Received (Total) – the total number of IP data packets received by the VPN Concentrator, including those received with errors.

Packets Received (Delivered) – the number of IP data packets received and successfully delivered to IP user protocols (including ICMP) on the VPN Concentrator; i.e., the VPN Concentrator was the final destination.

Packets Forwarded – the number of IP data packets received and forwarded to destinations other than the VPN Concentrator.

Outbound Packets with No Route – the number of outbound IP data packets discarded because no route could be found to transmit them to their destination. This number includes any packets that the VPN Concentrator could not route because all of its default routers are down.

Packets Transmitted (Requests) – the number of IP data packets that local IP user protocols (including ICMP) supplied to transmission requests. This number does not include any packets counted in Packets Forwarded.

Fragments Needing Reassembly – the number of IP fragments received by the VPN Concentrator that needed to be reassembled.

Reassembly Successes – the number of IP data packets successfully reassembled.

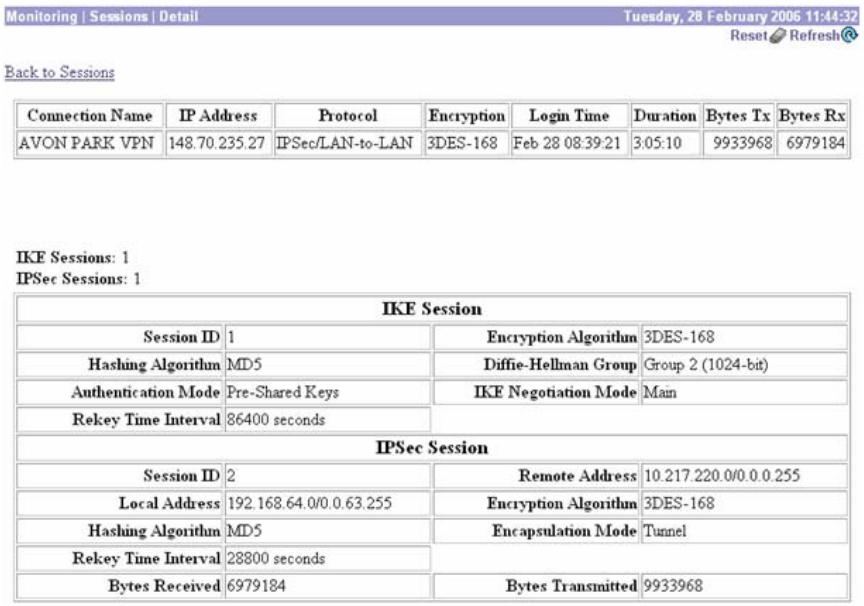
Reassembly Failures – the number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). This number is not necessarily a count of discarded IP fragments since

some algorithms can lose track of the number of fragments by combining them as they are received.

Fragmentation Successes – the number of IP data packets that have been successfully fragmented by the VPN Concentrator.

Fragmentation Failures – the number of IP data packets that have been discarded because they needed to be fragmented but could not be fragmented (for example, because the Don't Fragment flag was set).

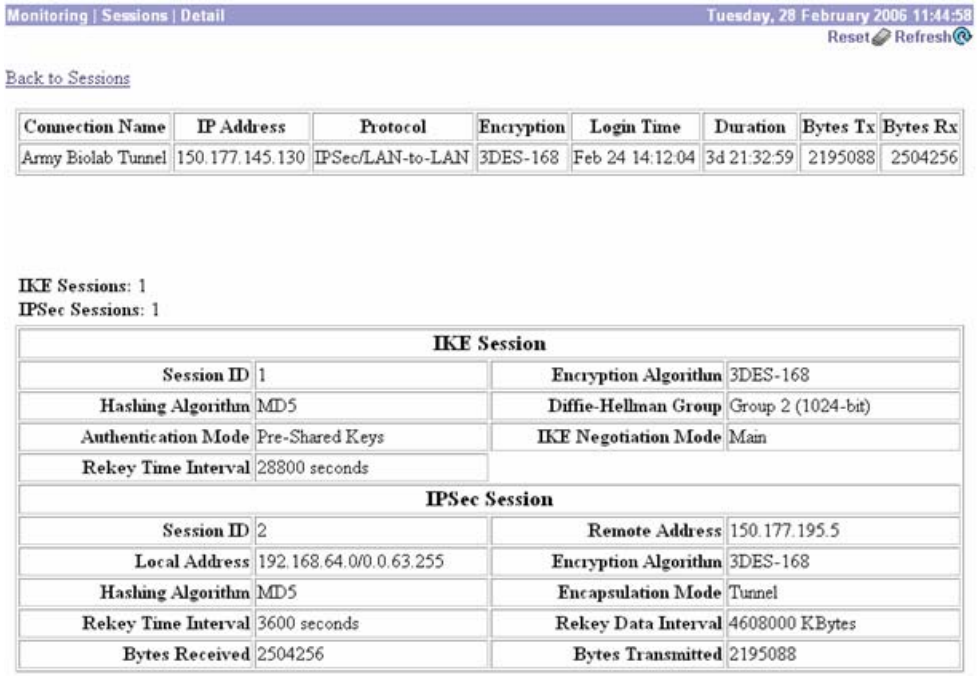
Fig-26 through Fig-28 indicates the Session Details for the active sessions during TNT 06-2. Use of this screen was important in order that one view of the critical circuit details, both parameters and statistics, could be viewed.



Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
AVON PARK VPN	148.70.235.27	IPSec/LAN-to-LAN	3DES-168	Feb 28 08:39:21	3:05:10	9933968	6979184

IKE Session			
Session ID	1	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Main
Rekey Time Interval	86400 seconds		
IPSec Session			
Session ID	2	Remote Address	10.217.220.0/0.0.0.255
Local Address	192.168.64.0/0.0.63.255	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Encapsulation Mode	Tunnel
Rekey Time Interval	28800 seconds		
Bytes Received	6979184	Bytes Transmitted	9933968

Figure 28. Manager Session Details (Avon Park)



Monitoring | Sessions | Detail — Tuesday, 28 February 2006 11:44:58

Reset Refresh

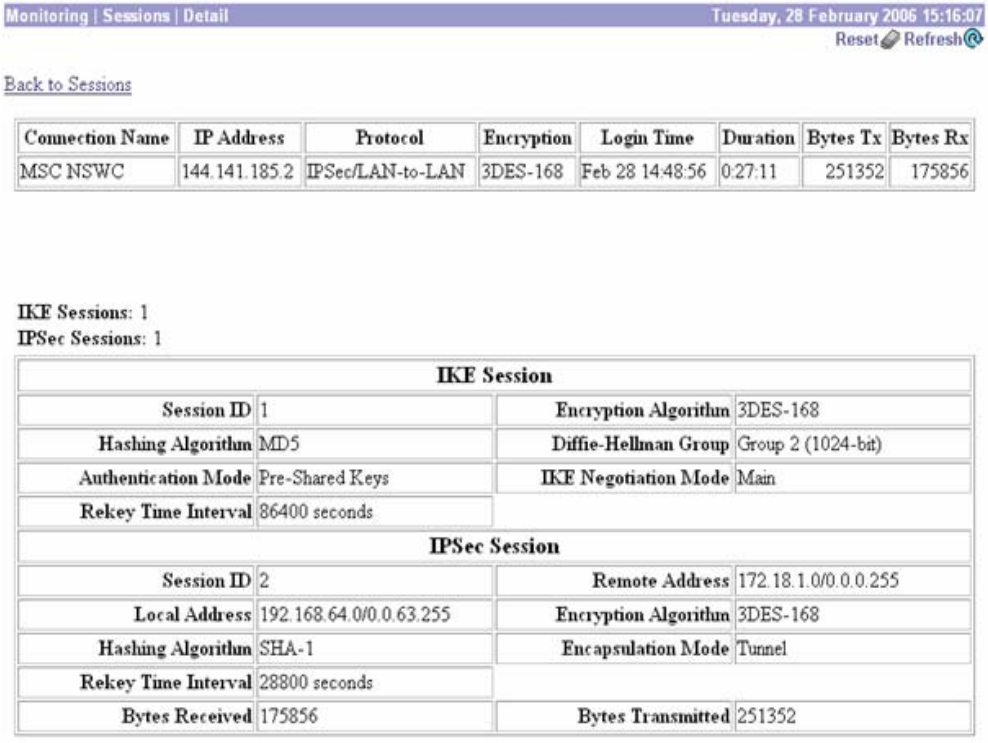
Back to Sessions

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
Army Biolab Tunnel	150.177.145.130	IPSec/LAN-to-LAN	3DES-168	Feb 24 14:12:04	3d 21:32:59	2195088	2504256

IKE Sessions: 1
IPSec Sessions: 1

IKE Session			
Session ID	1	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Main
Rekey Time Interval	28800 seconds		
IPSec Session			
Session ID	2	Remote Address	150.177.195.5
Local Address	192.168.64.0/0.0.63.255	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Encapsulation Mode	Tunnel
Rekey Time Interval	3600 seconds	Rekey Data Interval	4608000 KBytes
Bytes Received	2504256	Bytes Transmitted	2195088

Figure 29. Manager Session Details (BFC)



Monitoring | Sessions | Detail — Tuesday, 28 February 2006 15:16:07

Reset Refresh

Back to Sessions

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
MSC NSWC	144.141.185.2	IPSec/LAN-to-LAN	3DES-168	Feb 28 14:48:56	0:27:11	251352	175856

IKE Sessions: 1
IPSec Sessions: 1

IKE Session			
Session ID	1	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Main
Rekey Time Interval	86400 seconds		
IPSec Session			
Session ID	2	Remote Address	172.18.1.0/0.0.0.255
Local Address	192.168.64.0/0.0.63.255	Encryption Algorithm	3DES-168
Hashing Algorithm	SHA-1	Encapsulation Mode	Tunnel
Rekey Time Interval	28800 seconds		
Bytes Received	175856	Bytes Transmitted	251352

Figure 30. Manager Session Details (MSC)

(5) Experiment 5, Scenario 1, 28-Feb-06.

LAN-to-LAN Sessions [Remote Access Sessions | Management Sessions]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
AVON PARK VPN	148.70.235.27	IPSec/LAN-to-LAN	3DES-168	Mar 1 11:50:23	0:02:5	11096	49528
Army Biolab Tunnel	150.177.145.130	IPSec/LAN-to-LAN	3DES-168	Mar 1 7:43:42	4:09:3	4351848	1152496
MSC NSWC	144.141.185.2	IPSec/LAN-to-LAN	3DES-168	Feb 28 14:48:56	21:04:2	1472136	301232

Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token
rroth	172.16.1.1	NPSTNT06VPN	IPSec/NAT-T	Mar 1 10:57:49	WinNT	1179552	N/A

Figure 31. TNT 06-2 Observations (28Feb06)

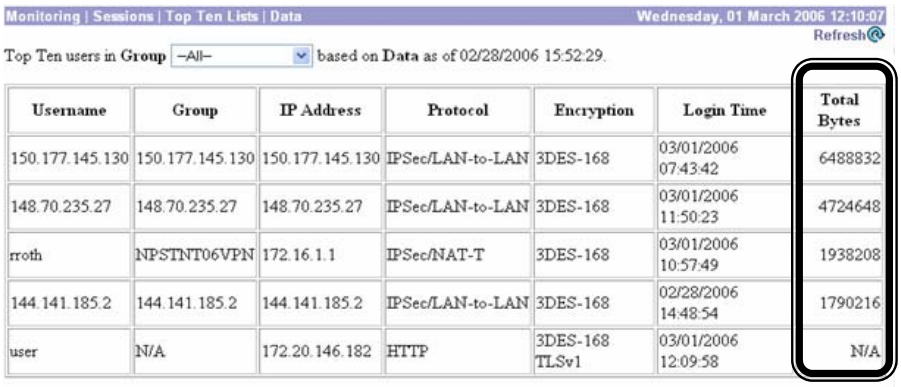
Monitoring | Statistics | MIB-II | IP — Tuesday, 28 February 2006 15:33:44

Reset Refresh

Packets Received (Total)	1292202
Packets Received (Header Errors)	58
Packets Received (Address Errors)	0
Packets Received (Unknown Protocols)	0
Packets Received (Discarded)	0
Packets Received (Delivered)	855391
Packets Forwarded	420575
Outbound Packets Discarded	0
Outbound Packets with No Route	1299
Packets Transmitted (Requests)	86926
Fragments Needing Reassembly	5534
Reassembly Successes	2767
Reassembly Failures	0
Fragmentation Successes	2707
Fragmentation Failures	0
Fragments Created	5414

Figure 32. TNT 06-2 Observations (28Feb06)

(6) Experiment 5, Scenario 2, 1-Mar-06.



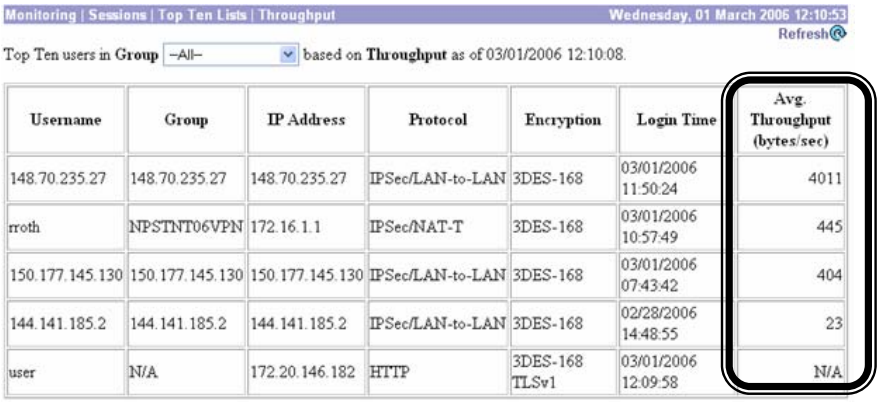
Monitoring | Sessions | Top Ten Lists | Data — Wednesday, 01 March 2006 12:10:07

Refresh

Top Ten users in **Group** –All– based on **Data** as of 02/28/2006 15:52:29.

Username	Group	IP Address	Protocol	Encryption	Login Time	Total Bytes
150.177.145.130	150.177.145.130	150.177.145.130	IPSec/LAN-to-LAN	3DES-168	03/01/2006 07:43:42	6488832
148.70.235.27	148.70.235.27	148.70.235.27	IPSec/LAN-to-LAN	3DES-168	03/01/2006 11:50:23	4724648
rroth	NPSTNT06VPN	172.16.1.1	IPSec/NAT-T	3DES-168	03/01/2006 10:57:49	1938208
144.141.185.2	144.141.185.2	144.141.185.2	IPSec/LAN-to-LAN	3DES-168	02/28/2006 14:48:54	1790216
user	N/A	172.20.146.182	HTTP	3DES-168 TLSv1	03/01/2006 12:09:58	N/A

Figure 33. TNT 06-2 Observations (1Mar06)



Monitoring | Sessions | Top Ten Lists | Throughput — Wednesday, 01 March 2006 12:10:53

Refresh

Top Ten users in **Group** –All– based on **Throughput** as of 03/01/2006 12:10:08.

Username	Group	IP Address	Protocol	Encryption	Login Time	Avg. Throughput (bytes/sec)
148.70.235.27	148.70.235.27	148.70.235.27	IPSec/LAN-to-LAN	3DES-168	03/01/2006 11:50:24	4011
rroth	NPSTNT06VPN	172.16.1.1	IPSec/NAT-T	3DES-168	03/01/2006 10:57:49	445
150.177.145.130	150.177.145.130	150.177.145.130	IPSec/LAN-to-LAN	3DES-168	03/01/2006 07:43:42	404
144.141.185.2	144.141.185.2	144.141.185.2	IPSec/LAN-to-LAN	3DES-168	02/28/2006 14:48:55	23
user	N/A	172.20.146.182	HTTP	3DES-168 TLSv1	03/01/2006 12:09:58	N/A

Figure 34. TNT 06-2 Observations (1Mar06)

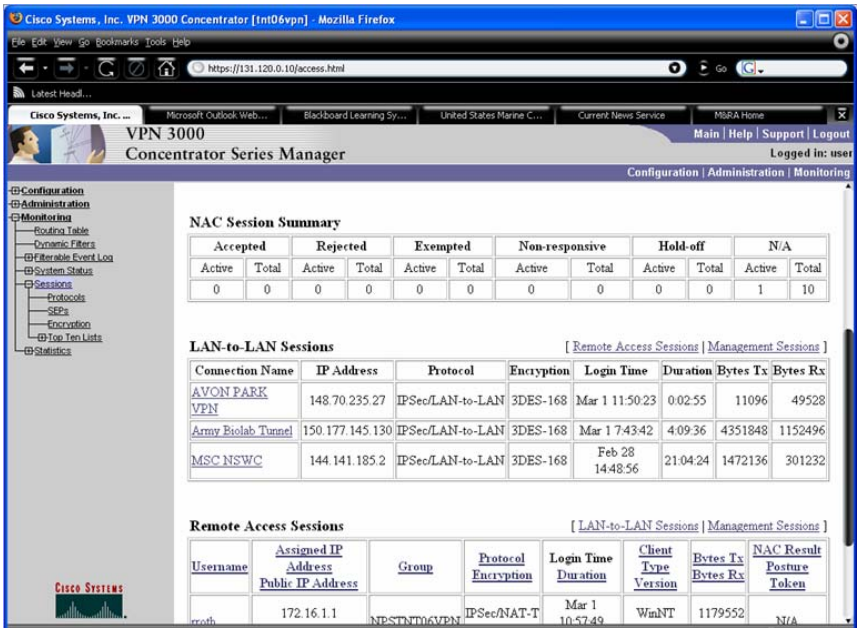


Figure 35. TNT 06-2 Observations (1Mar06)

(7) Experiment 5, Repeat Scenario 2, 2-Mar-06.

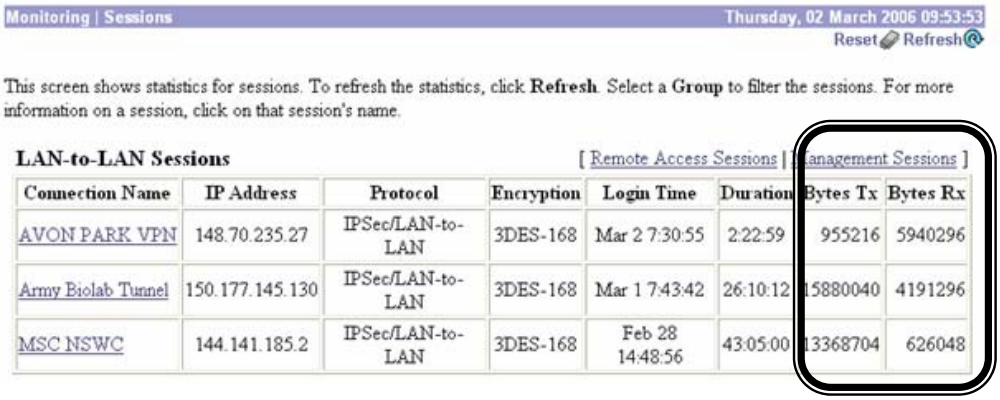
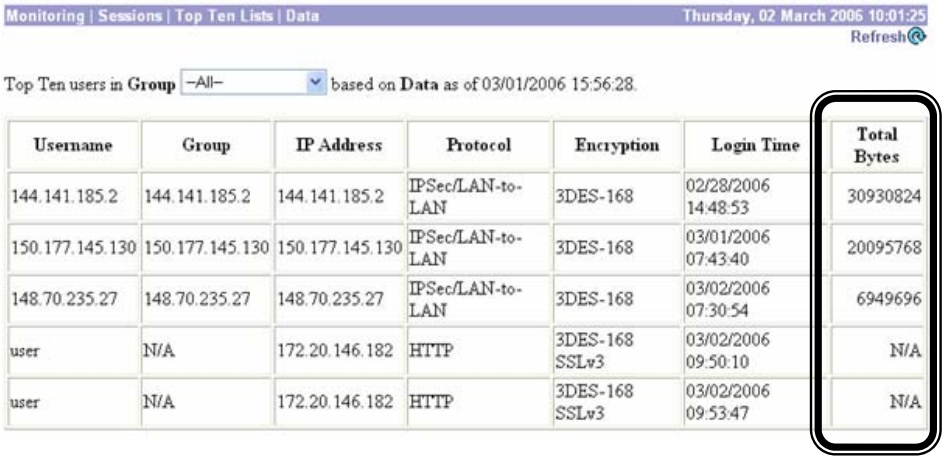


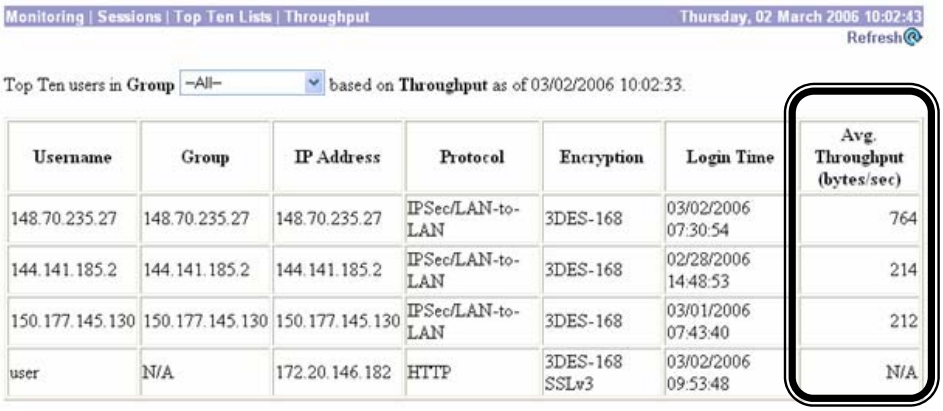
Figure 36. TNT 06-2 Observations (2Mar06)


Monitoring | Sessions | Top Ten Lists | Data — Thursday, 02 March 2006 10:01:25 — Refresh

Top Ten users in **Group** –All– based on **Data** as of 03/01/2006 15:56:28.

Username	Group	IP Address	Protocol	Encryption	Login Time	Total Bytes
144.141.185.2	144.141.185.2	144.141.185.2	IPSec/LAN-to-LAN	3DES-168	02/28/2006 14:48:53	30930824
150.177.145.130	150.177.145.130	150.177.145.130	IPSec/LAN-to-LAN	3DES-168	03/01/2006 07:43:40	20095768
148.70.235.27	148.70.235.27	148.70.235.27	IPSec/LAN-to-LAN	3DES-168	03/02/2006 07:30:54	6949696
user	N/A	172.20.146.182	HTTP	3DES-168 SSLv3	03/02/2006 09:50:10	N/A
user	N/A	172.20.146.182	HTTP	3DES-168 SSLv3	03/02/2006 09:53:47	N/A

Figure 37. TNT 06-2 Observations (2Mar06)


Monitoring | Sessions | Top Ten Lists | Throughput — Thursday, 02 March 2006 10:02:43 — Refresh

Top Ten users in **Group** –All– based on **Throughput** as of 03/02/2006 10:02:33.

Username	Group	IP Address	Protocol	Encryption	Login Time	Avg. Throughput (bytes/sec)
148.70.235.27	148.70.235.27	148.70.235.27	IPSec/LAN-to-LAN	3DES-168	03/02/2006 07:30:54	764
144.141.185.2	144.141.185.2	144.141.185.2	IPSec/LAN-to-LAN	3DES-168	02/28/2006 14:48:53	214
150.177.145.130	150.177.145.130	150.177.145.130	IPSec/LAN-to-LAN	3DES-168	03/01/2006 07:43:40	212
user	N/A	172.20.146.182	HTTP	3DES-168 SSLv3	03/02/2006 09:53:48	N/A

Figure 38. TNT 06-2 Observations (2Mar06)

- A limited amount of observations were made using SolarWinds Network Management Tool; due to the administrative limitations imposed on students and staff by NPS ITACS. The use of SolarWinds in capturing the movement of data packets, network failures, and various other administrative measures in future has been mitigated due to submission of a Change Configuration Board Request dated 27-Feb-06 and subsequent approval on 6-Mar-06. This request gave administrative control to the CENETIX personnel for future changes, in the daily operation and preparation of future TNT experiments.
- Once SNMP was enabled, via ITACS assistance, we could then track Network Performance through use of SNMP. The following figures were gathered during TNT 06-2, and focused primarily on the measurement of traffic across the link.

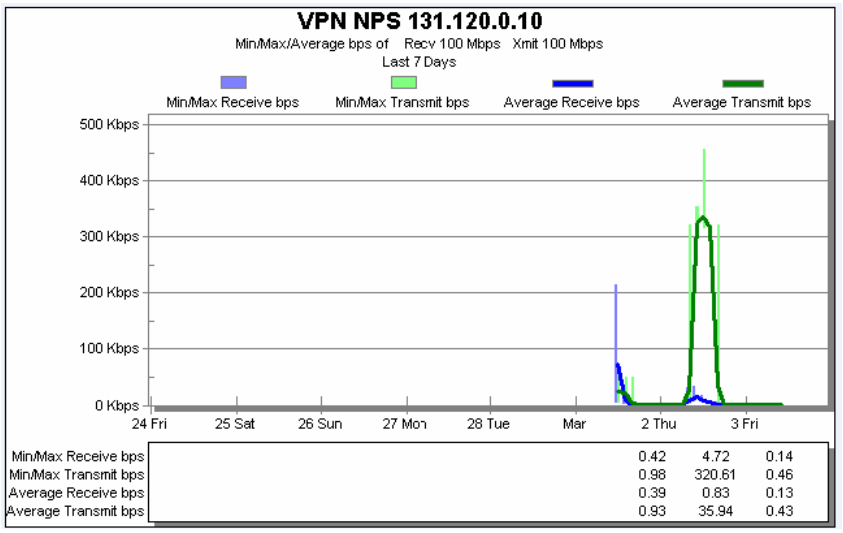


Figure 39. TNT 06-2 Solar Wind Observations- Avg bps

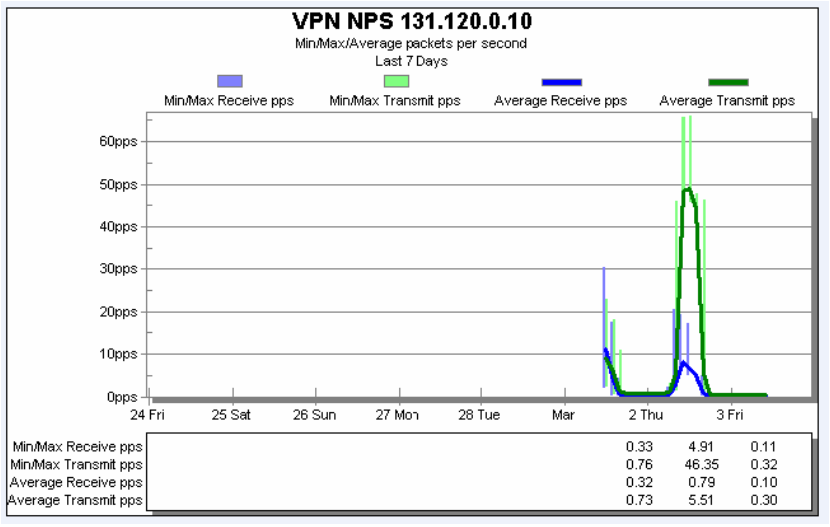


Figure 40. TNT 06-2 Solar Winds Observations – Avg pps

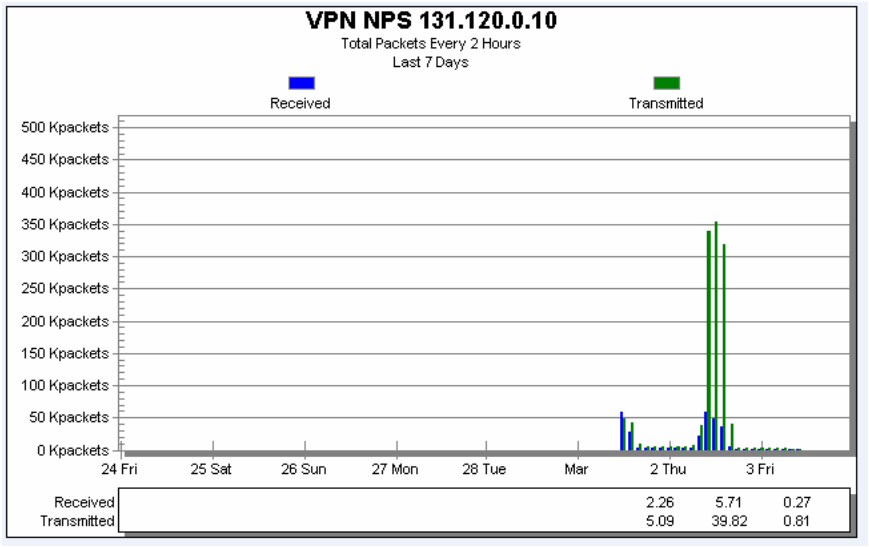


Figure 41. TNT 06-2 Solar Winds Observations – Total Packets

2. Recommendations

a. SNMP Configuration

Prior to the start of TNT 06-2 SNMP was not enabled, due to administrative constraints imposed by NPS ITACS. This restriction is enforced by ITACS to prevent students, who participate in this environment, from making unauthorized changes. On multiple occasions requesting SNMP to be enabled on the TNT VPN device was ignored, however ITACS ultimately enabled SNMP which allowed the CENETIX NOC to use SolarWinds in network monitoring of the VPN circuit on a limited scale.

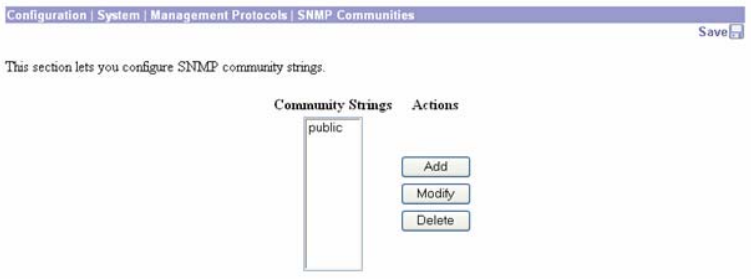


Figure 42. SNMP Manager Setting

b. Routing Tables

Problem statement: The BFC lost connection to the VPN, on 2-Mar-06, after a change to the Avon Park circuit. It is believed that the BFC could not gain access due to a problem with the routing table or ACL's.

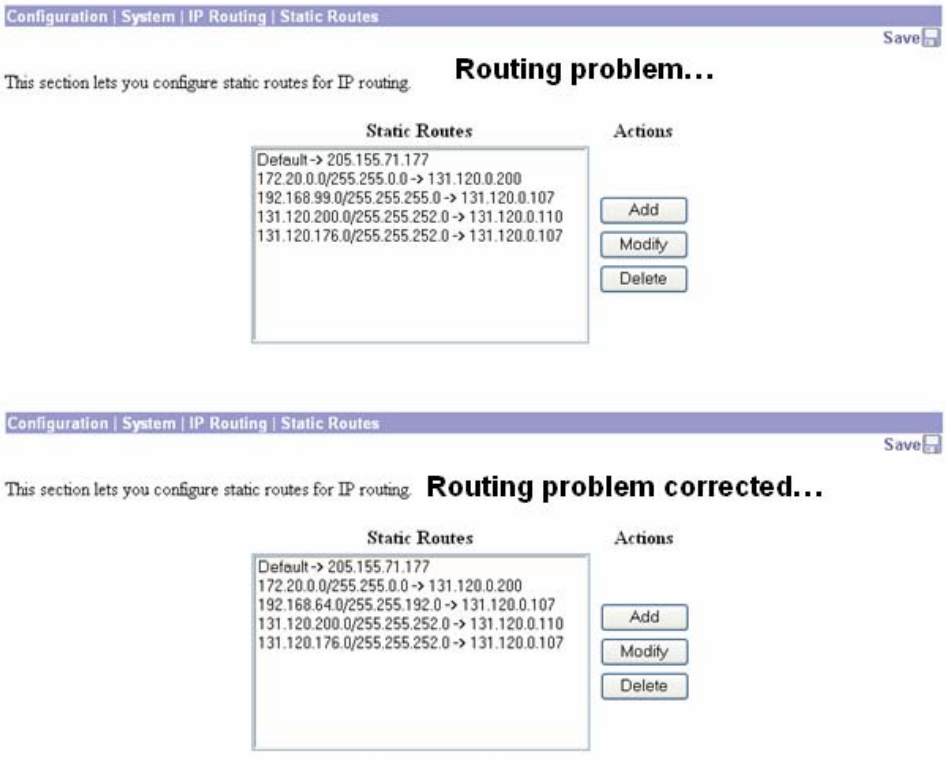


Figure 43. 3015 Static Route Table

Problem Resolution: This was required because all the 131 range of IPs was striped off of the ACL's, in order that the BFC could gain access to the CENETIX network. I believe this problem was caused by when Avon Park was configured for access on the concentrator.

c. Security Association (SA)

- A security association contains all of the information necessary for implementing the security services for a connection, such as the use of AH and ESP, the connection mode (tunnel or transport), the HMAC functions and encryption

algorithms, the keys to use for these functions and algorithms, the lifetime of the SA, and many other items.

- RFC 2402 – Authentication Header (AH) performs three main functions: data integrity services, data authentication, and protection against data replay attacks.
- AH protects the entire packet with the exception of TTL and TOS fields in the IP header.
- AH is a protocol like IP, ICMP, TCP and UDP. It is assigned the protocol number 51.
- RFC 2406 – Encapsulation Security Protocol (ESP) performs the same services as AH, but with two exceptions.
- ESP is a protocol like IP, ICMP, TCP and UDP. It is assigned the protocol number 50, and it layer Layer-3 protection of data.
- Provides encryption of the user data.
- ESP’s data authentication and integrity service only include the ESP header and payload – so if someone modified the ESP payload, ESP wouldn’t detect it, whereas AH would.
- For both the MSC and BFC we experienced problems with the Security Association piece of VPN. SA is basically a group of the necessary security components to successfully build a secure connection with an IPsec peer. VPNs accomplish this security process through two separate phases which it must successfully negotiate in order to construct a secure tunnel using IPsec.
- What may have caused this to fail during the site-to-site (L2L) VPN connection could have been caused by the Perfect Forward Secrecy was enabled. With this being set it caused a Phase 2 authentication failure with the SA IPsec proposals.

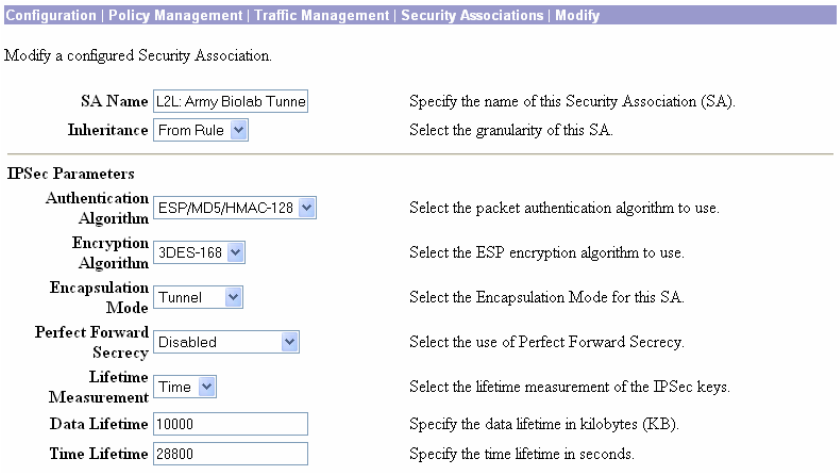


Figure 44. 3015 Perfect Forward Secrecy Setting

3. Tracking the Cisco VPN MIBs

Plans were made to track the following Cisco VPN MIBs during TNT 06-2; it was not until near the end of the experiment when ITACS finally allowed CENETIX NOC the opportunity to enable SNMP on the Cisco 3015 VPN Concentrator.

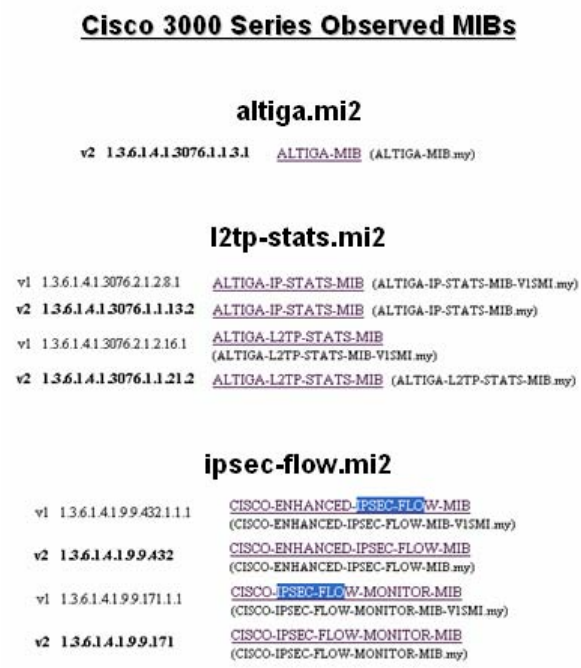
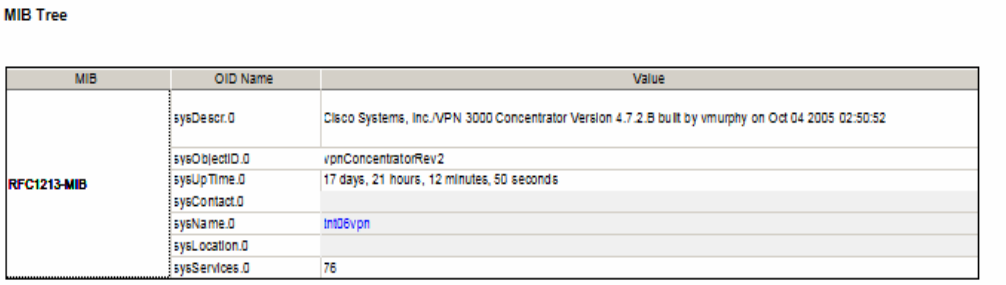


Figure 45. MIB-II Variables (A Few)

a. Problem with Tracking MIBs

On 3Mar06 CENETIX Lab; along with a significant portion of NPS lost power due to inclement weather. We had set SolarWinds to walk the MIB Trees for the above listed MIBs, but lost the track of data that SolarWinds would have captured for our use. The below is a depiction of what one MIB would have tracked (altiga.mi2).


MIB Tree

MIB	OID Name	Value
RFC1213-MIB	sysDescr.0	Cisco Systems, Inc./VPN 3000 Concentrator Version 4.7.2.B built by vmurphy on Oct 04 2005 02:50:52
	sysObjectID.0	vpnConcentratorRev2
	sysUpTime.0	17 days, 21 hours, 12 minutes, 50 seconds
	sysContact.0	
	sysName.0	tnt06vpn
	sysLocation.0	
	sysServices.0	76

Figure 46. Solar Winds MIB-11 Tree

4. Improvements to the TNT NOC

- Isolate the TNT Private VLAN and VPN Concentrator; in order that students/staff can administer with minimal ITACS support.
- Establish a class on SolarWinds/Orion and how to complete basic network management set-up, in preparation for TNT experiments and NOC student operations.
- Develop a lesson on what the various charts and graphs those are available in SolarWinds/Orion, and what the data that is displayed means.
- Incorporate a VTC between NOC-TOC at the beginning of the day, and end of the day in order that plans can be deconflicted or adjusted as needed. This way both the NOC and TOC understand the goals/results were for the day.
- Develop Business Plans directing units who desire to operate on CENETIX network.
- Ensure that CENETIX NOC has as many administrative privileges as possible without conflicting with ITACS policies. If authorization to make administrative changes

would be granted to a few personnel (Mike Clement, Eugene Boukarov, Dr. Bordetsky) they could make appropriate changes to the CENETIX Testbed, as required.

B. TNT 06-3

From 13-14 June 2006, NPS faculty and students continued experiments to evaluate the use of networks, advanced sensors, and collaborative technology for rapid Maritime Interdiction Operations (MIO); specifically the ability for a Boarding Party to rapidly set-up ship-to-ship communications that permit connectivity with C2 organizations, and collaborating with remotely located sensor experts.

The experiment extends the number of participating organizations beyond the TNT 06-2 MIO to include two international teams in Sweden and Austria, as well as the San Francisco Police Department (SFPD) and the Alameda County Marine Units.

1. Architecture

Although the number of participants who required a L2L connection decreased during this experiment, the use of VPN Clients increased, and the need for using NAT-T for the first time was implemented. In the below figure, CGSA required the use of a Netgear Router which afforded them the ability to provide a layer of security between the Internet and their end users (Fig-45). Because this scenario required NAT-T, constructing the circuit to port forward and tunnel through their ISP was required. This scenario although challenging, was validated prior to commencing TNT 06-3.

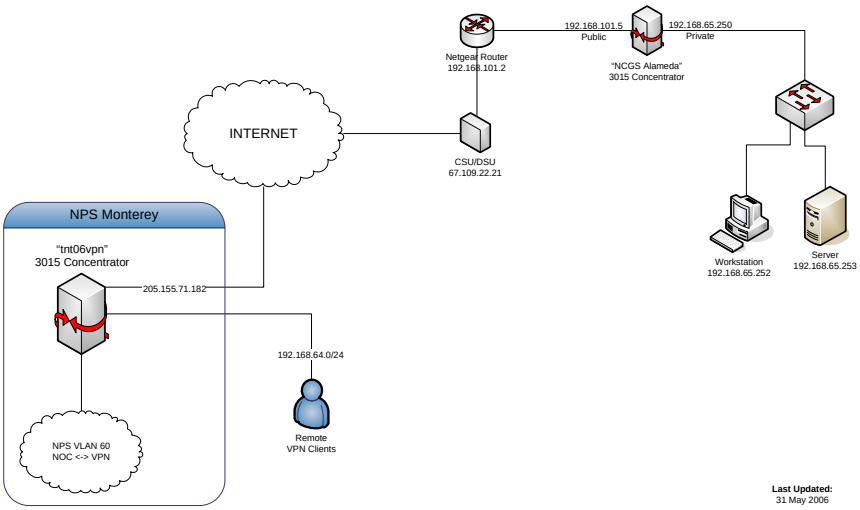


Figure 47. CGSA – VPN Scenario.

2. Configuration Details

a. Network Topology: On-Site Infrastructure

Over the past several iterations of experimentation, we have been implementing and utilizing VPN architecture for connecting the remote NOC at NPS, the local TOC and operational network in the Bay Area, and other interested parties such as LLNL and BFC participants in one private experimental network. This iteration, our communications requirements dictated the need for both a VPN connection in order to access NPS NOC resources and to allow for remote network monitoring via SolarWinds and similar tools, and a standard Internet connection in order to access the NPS-owned Groove server, providing the backend for our collaborative environment.

Due to the learning curve in building site-to-site (L2L) VPN connections via NAT-T, we experimented with a number of topological options before finding the best fit for our circumstances at CGSA. Initially, we implemented

parallel connections over two distinct Internet connections provided at CGSA, utilizing a DSL connection for Internet and a T1 for VPN. The initial topology was as follows:

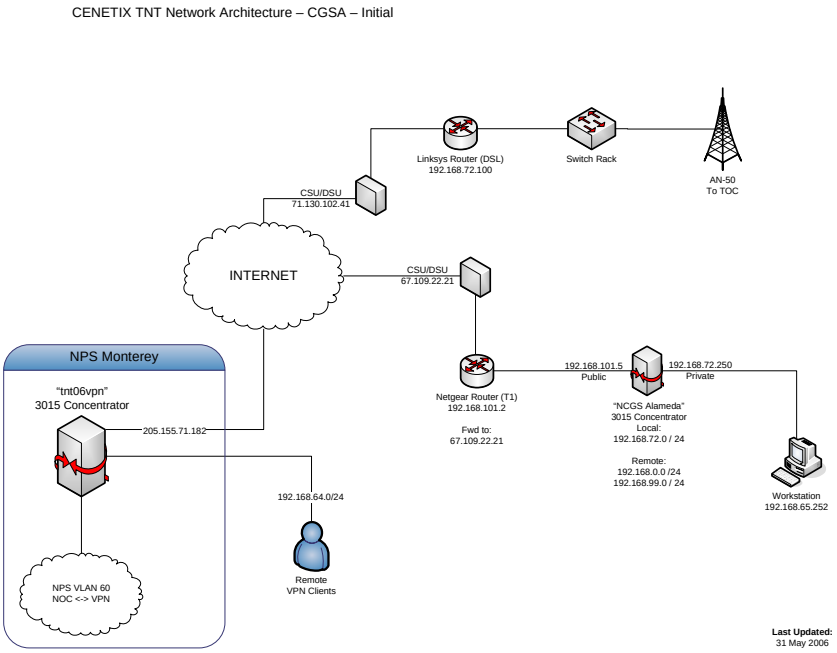


Figure 48. CGSA Initial Topology.

All client computers in the primary local network had addresses of the form 192.168.72.xxx, with a 24-bit (255.255.255.0) netmask. Their default gateway was set to 192.168.72.100, the address of the Linksys DSL router. The DSL router had static routes set to redirect VPN-bound traffic back through the local network to the Cisco concentrator and onward toward remote sites. This provided standard Internet connectivity as well as VPN connectivity for remote sites. The Netgear router provided a NAT service, and so we configured port forwarding for TCP and UDP ports 500, 4500, and 10,000 to the public interface of the concentrator, in order to allow proper VPN functionality.

However, we experienced a number of problems with this configuration:

- Address Conflicts: The Linksys DSL router was configured with a small DHCP segment in order to support USCG internal users on the same network. Before we established a preliminary IP plan, we were inadvertently assigning IP addresses that conflicted with DHCP addresses.
- Redirect Overload: Since the default gateway specified for all nodes was the DSL router, it was responsible for reflecting all traffic destined for the VPN back into the local network toward the concentrator. This put additional stress on the router, and decreased overall network performance for both Internet and VPN access.
- Unstable Platform: The DSL router, possibly due to the combination of the above afflictions, began to sporadically fail, requiring a full power cycle. This would happen as often as once every 10 to 15 minutes, resulting in a largely unusable configuration. The exact cause and prognosis were never determined.

In order to solve these issues, we experimented with configuring the VPN concentrator itself as a normal Internet router, which turned out to be nearly its default configuration. The only lack of capability of the concentrator was to perform NAT, a function which was taken on by the Netgear router connecting the concentrator to the T1 line. By changing the default filters on the concentrator’s public interface to allow all traffic through, it began to route standard Internet traffic as easily as it did VPN traffic. The resulting configuration was as follows:

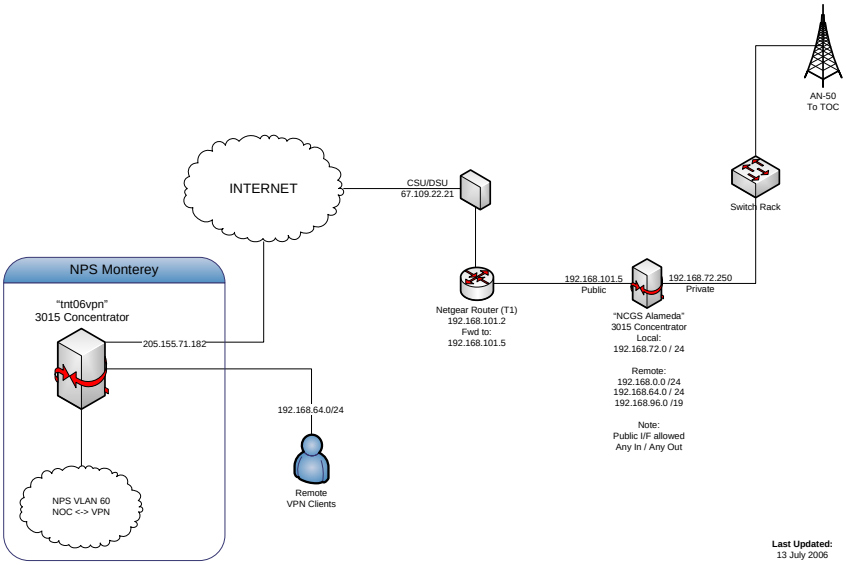


Figure 49. CGSA – NAT Configuration.

We changed every computer's default gateway to use 192.168.72.250, which resulted in all users utilizing the VPN concentrator to forward all traffic. This provided acceptable performance and stability for the remainder of the experiment. We also changed the VPN tunnel-able networks to include a broader range of IP addresses for additional subnets in the Bay Area, to cover more of the IP space dedicated to the NOC, and to support the range of VPN software clients.

b. Network Topology: Global VPN Infrastructure

Beyond the Bay Area infrastructure, we utilized VPN architecture to connect various experimental sites, including the NPS campus, Ulrich Wagner's team in Austria, and various one-off software clients, such as from LLNL. All connections terminated at NPS, which acted as the central relay point for all sites. We did not notice any performance drawbacks to this design; however, for future

performance and reliability concerns we could consider directly connecting all remote VPN sites to the Bay Area (i.e., Coast Guard Island) VPN concentrator.

The global VPN infrastructure ultimately appeared as follows:

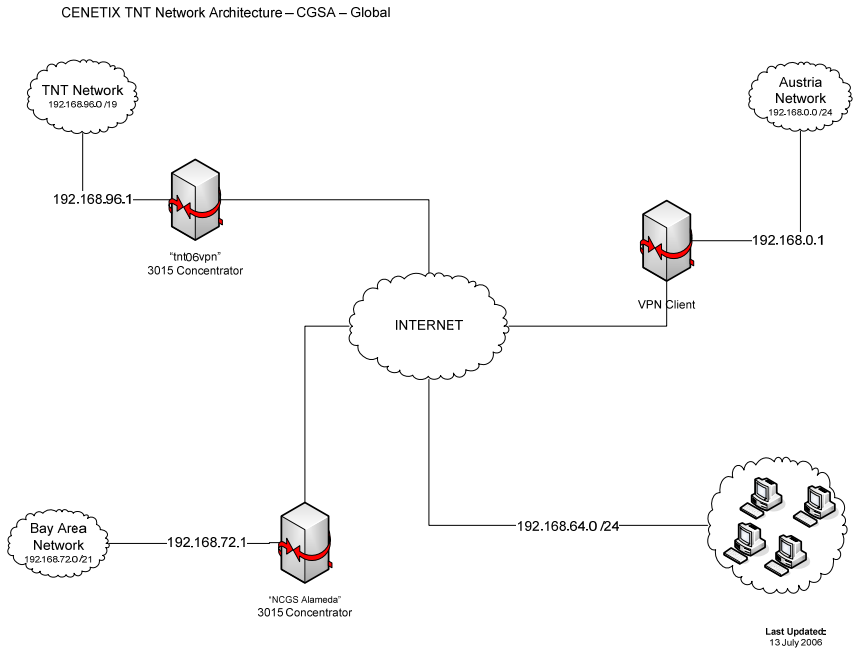


Figure 50. CGSA – Global VPN Infrastructure.

3. Observations

Prior to TNT 06-3, several attempts were made to configure the Concentrator from my home (761CTNWD) and ultimately success was achieved once the port forwarding aspect of the router was configured. Attempting to simulate, as nearly as possible, the equipment string that would be implemented at CGSA, the following architecture was tested.

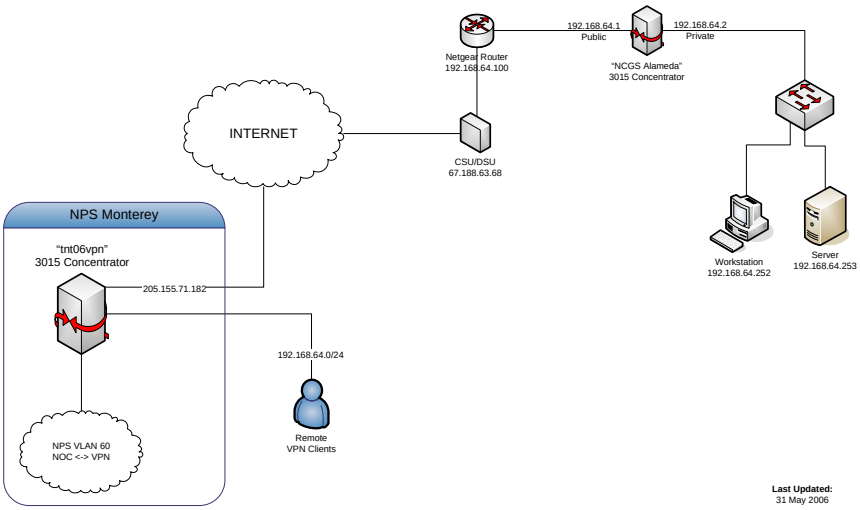


Figure 51. CGSA – Testbed from 761CTNWD.

Using my Motorola Router, and my ISP Comcast, I was able to simulate the VPN configuration we would require for TNT 06-3 at CGSA. As stated earlier in Chapter II (IPsec and Firewalls), configuring NAT-T to tunnel through allowed a NAT-T connection to be established, as seen in the below figure.

```
562 05/30/2006 14:00:17.200 SEV=5 IKE/66 RPT=33 67.188.63.68
Group [67.188.63.68]
IKE Remote Peer configured for SA: L2L: 761CTNWD_NPS

563 05/30/2006 14:00:17.260 SEV=4 IKE/173 RPT=8 67.188.63.68
Group [67.188.63.68]
NAT-Traversal successfully negotiated!
IPSec traffic will be encapsulated to pass through NAT devices.

566 05/30/2006 14:00:17.260 SEV=4 IKE/49 RPT=33 67.188.63.68
Group [67.188.63.68]
Security negotiation complete for LAN-to-LAN Group (67.188.63.68)
Responder, Inbound SPI = 0x1880a5e2, Outbound SPI = 0x3b1705ac

569 05/30/2006 14:00:17.270 SEV=4 IKE/120 RPT=33 67.188.63.68
Group [67.188.63.68]
PHASE 2 COMPLETED (msgid=b3c6e837)
```

Figure 52. NAT-T Log – Testbed from 761CTNWD.

During the experiment, the following observations were made:

LAN-to-LAN Sessions [Remote Access Sessions | Management Sessions]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
CGSA	67.109.22.21	IPSec/LAN-to-LAN/NAT-T	3DES-168	Jun 14 11:56:21	2:24:56	78336744	200461768
Utech	84.145.13.4	IPSec/LAN-to-LAN	AES-128	Jun 14 13:51:57	0:29:20	87664	58896

Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address / Public IP Address	Group	Protocol / Encryption	Login Time / Duration	Client Type / Version	Bytes Tx / Bytes Rx	NAC Result / Posture Token
adougan3	192.168.64.1 128.115.186.238	NPSTNT06VPN	IPSec 3DES-168	Jun 14 10:31:51 3:49:26	WinNT 4.8.00.0440	25898520 2711840	N/A
adougan2	192.168.64.4 128.115.198.103	NPSTNT06VPN	IPSec 3DES-168	Jun 13 12:33:52 25:47:26	WinNT 4.6.01.0019	11271184 17797320	N/A
adougan	192.168.64.2 128.115.198.69	NPSTNT06VPN	IPSec 3DES-168	Jun 13 11:50:12 26:31:06	WinNT 4.6.02.0011	322216 312656	N/A
adougan4	192.168.64.3 128.115.186.97	NPSTNT06VPN	IPSec 3DES-168	Jun 13 12:11:42 26:09:37	WinNT 4.6.01.0019	92890648 3408128	N/A
farrellmm	192.168.64.5 67.160.195.107	NPSTNT06VPN	IPSec/NAT-T 3DES-168	Jun 14 14:19:37 0:01:40	WinNT 4.6.02.0011	83096 78704	N/A
hanzvola	192.168.64.6 84.217.41.223	NPSTNT06VPN	IPSec/NAT-T 3DES-168	Jun 14 11:16:20 3:04:58	WinNT 4.6.02.0011	99374488 16814776	N/A

Figure 53. L2L and Remote Connections TNT 06-3.

Monitoring | Sessions | Top Ten Lists | Data — Wednesday, 14 June 2006 14:25:32

Refresh

Top Ten users in **Group** –All– based on **Data** as of 06/13/2006 13:25:36.

Username	Group	IP Address	Protocol	Encryption	Login Time	Total Bytes
67.109.22.21	67.109.22.21	67.109.22.21	IPSec/LAN-to-LAN/NAT-T	3DES-168	06/14/2006 11:56:22	279116744
adougan4	NPSTNT06VPN	192.168.64.3	IPSec	3DES-168	06/13/2006 12:11:41	96335032
adougan2	NPSTNT06VPN	192.168.64.4	IPSec	3DES-168	06/13/2006 12:33:52	29099632
adougan3	NPSTNT06VPN	192.168.64.1	IPSec	3DES-168	06/14/2006 10:31:52	28695736
adougan	NPSTNT06VPN	192.168.64.2	IPSec	3DES-168	06/13/2006 11:50:12	635872
farrellmm	NPSTNT06VPN	192.168.64.5	IPSec/NAT-T	3DES-168	06/14/2006 14:19:38	212624
84.145.13.4	84.145.13.4	84.145.13.4	IPSec/LAN-to-LAN	AES-128	06/14/2006 13:51:58	168320
admin	N/A	192.168.64.5	HTTP	3DES-168 SSLv3	06/14/2006 14:21:11	N/A

Figure 54. Data: Total Bytes TNT 06-3.

Monitoring | Sessions | Top Ten Lists | Duration — Wednesday, 14 June 2006 14:25:57

Refresh

Top Ten users in **Group** –All– based on **Duration** as of 06/14/2006 14:25:32.

Username	Group	IP Address	Protocol	Encryption	Login Time	Duration
adougan	NPSTNT06VPN	192.168.64.2	IPSec	3DES-168	06/13/2006 11:50:11	26:35:46
adougan4	NPSTNT06VPN	192.168.64.3	IPSec	3DES-168	06/13/2006 12:11:40	26:14:17
adougan2	NPSTNT06VPN	192.168.64.4	IPSec	3DES-168	06/13/2006 12:33:51	25:52:06
adougan3	NPSTNT06VPN	192.168.64.1	IPSec	3DES-168	06/14/2006 10:31:51	3:54:06
67.109.22.21	67.109.22.21	67.109.22.21	IPSec/LAN-to-LAN/NAT-T	3DES-168	06/14/2006 11:56:21	2:29:36
84.145.13.4	84.145.13.4	84.145.13.4	IPSec/LAN-to-LAN	AES-128	06/14/2006 13:51:57	0:34:00
farrellmm	NPSTNT06VPN	192.168.64.5	IPSec/NAT-T	3DES-168	06/14/2006 14:19:37	0:06:20
admin	N/A	192.168.64.5	HTTP	3DES-168 SSLv3	06/14/2006 14:21:10	0:04:47

Figure 55. Duration TNT 06-3.

Monitoring | Sessions | Top Ten Lists | Throughput — Wednesday, 14 June 2006 14:26:19

Refresh

Top Ten users in **Group** –All– based on **Throughput** as of 06/14/2006 14:25:32.

Username	Group	IP Address	Protocol	Encryption	Login Time	Avg. Throughput (bytes/sec)
67.109.22.21	67.109.22.21	67.109.22.21	IPSec/LAN-to-LAN/NAT-T	3DES-168	06/14/2006 11:56:21	31025
adougan3	NPSTNT06VPN	192.168.64.1	IPSec	3DES-168	06/14/2006 10:31:51	2039
adougan4	NPSTNT06VPN	192.168.64.3	IPSec	3DES-168	06/13/2006 12:11:40	1019
farrellmm	NPSTNT06VPN	192.168.64.5	IPSec/NAT-T	3DES-168	06/14/2006 14:19:37	598
adougan2	NPSTNT06VPN	192.168.64.4	IPSec	3DES-168	06/13/2006 12:33:51	312
84.145.13.4	84.145.13.4	84.145.13.4	IPSec/LAN-to-LAN	AES-128	06/14/2006 13:51:57	83
adougan	NPSTNT06VPN	192.168.64.2	IPSec	3DES-168	06/13/2006 11:50:11	6
admin	N/A	192.168.64.5	HTTP	3DES-168 SSLv3	06/14/2006 14:21:10	N/A

Figure 56. Average Throughput TNT 06-3.

4. Recommendations

Establish a proposed IP plan and network topology A comprehensive IP configuration for every anticipated node should be constructed, leaving space available for last-minute additions and changes. This includes not only node IP addresses, but the determination of subnetting and

gateway addresses. This listing should be distributed both via email prior to the experiment and by paper copy on the first day of configuration. Doing so not only enables all users to properly configure their nodes, but also to identify configuration problems and to allow shared knowledge of server and camera locations for easy access by users.

Since this also will change as the experiment progresses, it is important to maintain the standard IP address webpage. This will ensure that all users have a common point of reference for double-checking their IP addresses, de-conflicting, and finding the address of a desired server.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. FUTURE CONSIDERATIONS

A. FUTURE CONFIGURATION

1. Test Operations of SSL for TNT 06-4

Secure Socket Layer (SSL) began as a protocol to protect web-based (HTTP) traffic between an end-user device and a web server. However, in the case for the CENETIX Lab environment, it may be possible to implement SSL as a VPN solution for clients, with the main benefit being the software in the form of a web browser is already installed on client systems.

Two main differences between IPsec and SSL are: IPsec provides protection for IP packets and protocols transmitted between networks or hosts. While SSL VPNs, provide protection for users' access to services and applications on a network. (Deal, 157)

Because SSL VPN can typically support two methods of authentication: digital certificates, and username/password (or tokens), it is recommended that the later be utilized for clients who require SSL VPN connectivity.

When making the final decision in utilization of SSL VPNs, the following table should be considered: (Deal, 167-168)

Component	SSL	IPsec
Connectivity	SSL only supports remote access	IPsec supports both site-to-site and remote access
Device authentication	SSL supports digital certificates	IPsec supports pre-shared keys, RSA encrypted nonces, and digital certificates

Component	SSL	IPsec
User authentication	SSL supports user authentication	IPsec supports user authentication through XAUTH unless it's L2TP/IPsec, in which case it's L2TP that is responsible for user authentication
Protection	SSL protects only the TCP payload and is thus susceptible to certain kinds of attacks	IPsec can protect the user's data in a transport connection or an entire IP packet in tunnel mode
Encryption	SSL/TLS support RC2, RC4, IDEA, DES, 3DES, and AES; however most web browsers only support RC4, DES, and 3DES	IPsec supports DES, 3DES, and AES
Message integrity	SSL supports none except that provided by TCP	IPsec supports MD5 and SHA-1 HMAC functions
Implementation requirements	SSL requires a web browser with Java/ActiveX installed for thin and network clients; because a web browser is used, most user operating systems will be supported	IPsec requires an IPsec client installed or built into the operating system and configured on each user's desktop; because a special client must be installed, only operating systems supported by the vendor can use IPsec
Transparency	SSL has no problem with a session traversing an address translation device (NAT and/or PAT)	IPsec has problems with AH traversing through any type of address translation device and ESP traversing a PAT device; however, IPsec is more likely to be denied by a firewall than a TCP port 443 (SSL) connection
ISP issues	Because SSL is commonly used on the Internet, ISPs don't block this kind of traffic	Some ISPs block IPsec traffic and require users to pay an additional fee to use IPsec; you can get around this problem by encapsulating IPsec data in either a TCP or UDP segment, but this adds overhead to the transmission; this assumes that this process doesn't break the ISP's acceptable use policy (AUP)

Table 2. SSL and IPsec Comparison. (From: Deal, 167-168)

2. IP Plan

The management of IP addresses has proven to be the most critical aspect piece of IT management, and it is no different in regards to the experiments that are operating within the CENETIX infrastructure.

Currently the CENETIX testbed utilizes three subnets from the 192.168.0.0 private IP space.

192.168.99.xxx	CENETIX Lab
192.168.100.xxx	OFDM Backbone
192.168.112.xxx	Wireless ITT Mesh

Device addresses are then managed via a few network administrators, and then displayed on the TNT website in order that network users can validate changes or additions.

Figure 57. TNT Host IP Configuration

In coordination with other CENETIX NOC Administrators an IP addressing scheme was derived for consideration in regards to future configuration changes. These changes would allow for a more logical approach to the overall management and operation of the CENETIX infrastructure. By

defining the third octet of the 192.168.x.x IP space, administrative control could be more easily accomplished as providing a level of scalability for changes in order that additional devices could be quickly and accurately added.

The following recommendations are provided, in regards to IP address management:

IP Addressing Scheme for TNT network		
Overall IP space	192.168.64.0 / 255.255.192.0 (192.168.64.0 – 192.168.127.255)	
Proposed Reservations		
VPN remote sites	Address/Subnet Mask	Comments
	192.168.64.0 / 255.255.240.0 (192.168.64.0 – 192.168.79.255)	
	192.168.64.0 / 255.255.255.0	VPN software clients
	192.168.65.0 / 255.255.255.0	Alameda / LLNL OFDM extension
Unassigned – future VPN expansion	192.168.80.0 / 255.255.240.0 (192.168.80.0 – 192.168.95.255)	
Core VPN sites and infrastructure	192.168.96.0 / 255.255.240.0 (192.168.96.0 – 192.168.111.255)	
	192.168.96.0 / 255.255.255.0	PTP links and small infrastructure subnets
	192.168.96.0 / 255.255.255.240	NPS VPN to NPS NOC Router
	192.168.97.0 / 255.255.255.0	Reserved for Marina CIRPAS expansion
	192.168.98.0 / 255.255.255.0	Reserved for Camp Roberts expansion
	192.168.99.0 / 255.255.255.0	NPS CENETIX Lab (NOC)
	192.168.100.0 / 255.255.255.0	Monterey Bay / Salinas Valley OFDM
	192.168.101.0 – 192.168.111.255	Unassigned
Local Experimental Subnets	192.168.112.0 / 255.255.248.0 (192.168.112.0 – 192.168.119.255)	
	192.168.112.0 / 255.255.255.128	ITT Mesh Network #1
	192.168.112.128 / 255.255.255.128	ITT Mesh Network #2
	192.168.113.0 – 192.168.118.255	Unassigned
	192.168.119.0 / 255.255.255.0	Small vehicular subnets
	192.168.119.0 / 255.255.255.240	NPS UAV #1
	192.168.119.16 / 255.255.255.240	NPS UAV #2
Reserved Testing Subnets	192.168.120.0 / 255.255.248.0 (192.168.120.0 – 192.168.127.255)	

Figure 58. Proposed IP Address Management Scheme

Secondly, utilizing DHCP more frequently would alleviate the burden of an administrator managing IP addresses as well as removing the human element of error when assigning IP addresses. It is realized that routers and switches do not generally use DHCP, but some automation may be utilized through the use of TFTP. However, with workstations the use of a DHCP server should dynamically assign addresses, and thus stored on a DNS server for the efficiency of the network.

3. Purchase Additional 3000 Series Concentrators

With the growth of CENETIX Lab in the past four years, and the number of organizations that desire to participate, the 3000 Series Concentrators provide the scalability that is required for L2L connections, which the CENETIX Lab

would require. Due to the ease of configuration management, versus a PIX or ASA router, students and faculty could more easily configure the device for future growth. With future purchases, it is also possible to configure the device prior to any exercise (locally), and then ship to the participating organizations who desire a L2L connection.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

The opportunity to work with the CENETIX Lab provided a capstone to my instruction at NPS. Finding a Thesis project that would incorporate both Information Technology and Management was crucial to my decision when choosing this thesis topic.

The CENETIX Testbed has extended its reach beyond the Monterey Bay area and provided remote organizations a means to participate in experiments that will benefit the decision makers for those war fighters of the 21st century. By providing a means in supporting organizations, such as SOCOM, LLNL, BFC, etc, the means to observe these experiments in a collaborative manner will only perfect the final outcome.

Some of the questions that this thesis attempted to address when contemplating a VPN solution include:

- What is the confidence level of the data you are sending?
- What do I need to protect?
- What kind of protection is required?
- What value is placed on the secrecy?
- How important is it to know the source of received data?
- Is it scalable?
- What is the cost?

These questions only represent a very few that could be asked, but they do represent the more important questions that need to be addressed up front by those who manage and make decisions as an IT manager.

Furthermore, I attempted to address some of the major advantages of a VPN which include: Security, Deployment Advantages, and Cost Effectiveness. Of these, security is the most important IT requirement when considering and implementing in a VPN solution. As well as addressing the deployment advantages and cost effectiveness of a VPN solution, both from the economic advantages and ease in utilizing existing infrastructure in the installation of a VPN would be evident once the project was initiated.

Lastly, by addressing the observations that were experienced during TNT 06-2 and 06-3, future operations of the Cenetix Lab VPN solution can evolve to better meet the needs of its primary customers during future experiments. Possible future solutions involve implementing an effective IP management plan, SSL Web VPN, and extending the Cenetix Lab via additional purchases of the Cisco 3000 Series Concentrator.

LIST OF REFERENCES

Brown, Steven. Implement Virtual Private Networks. McGraw-Hill, May 1999.

Covill, Randall Jorde. Implementing Extranets: The Internet as a Virtual Private Network. Digital Press, September 1998.

CP-I, Cisco Press. VPN 3000 Series Concentrator Reference, Volume I: Configuration. Release 4.7, February 2005.

CP-II, Cisco Press. VPN 3000 Series Concentrator Reference, Volume II: Administration and Monitoring. Release 4.7, February 2005.

Deal, Richard. The Complete Cisco VPN Configuration Guide. Cisco Press, 2006.

Fowler, Dennis. Virtual private Networks: Making the Right Connection. Morgan Kaufmann Publishers, June 1999.

Goralski, Walter; Waclawski, David. Virtual Private Networks: Achieving Secure Internet Commerce and Enterprise-wide Communications Computer Technology Research Corporation, April 1999.

Mapquest. World Map and United States Map.

Ruixi Yuan, W. Timothy Strayer, Virtual Private Networks: Technologies and solutions" Addison-Wesley, April 2001.

Tiller, James S.; Tiller, Jim S. A Technical Guide to IpSec Virtual Private Networks. Auerbach Publications, December 2000.

TNT 06-2 and 06-3 Participants. After Action Comments.

Zeltser, Stephen; Winters, Scott; Ritchey, Ronald; Northcutt, Stephen; Kent, Karen. Inside Network Perimeter Security, 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education
   MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center
   MCCDC, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

7. Dan Boger
   Naval Postgraduate School
   Monterey, California